CrossTalk

Nov/Dec 2009 **The Journal of Defense Software Engineering** Vol. 22 No. 7

21st Century Defense

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **DEC 2009**	2. REPORT TYPE	3. DATES COVERED **00-11-2009 to 00-12-2009**
4. TITLE AND SUBTITLE **CrossTalk: The Journal of Defense Software Engineering. Volume 22, No. 7, Nov/Dec 2009**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **CrossTalk,517 SMXS/MXDEA,6022 Fir Ave,Hill AFB,UT,84056-5820**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR’S ACRONYM(S)
		11. SPONSOR/MONITOR’S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**		
13. SUPPLEMENTARY NOTES		
14. ABSTRACT		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT **Same as Report (SAR)**	18. NUMBER OF PAGES **32**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

21st Century Defense

Software Engineering Technology

Open Forum

On The Cover

Cover Design by
Kent Bingham

Departments

CrossTalk

OSD (AT&L)	*Kristen Baldwin*
NAVAIR	*Jeff Schwalb*
309 SMXG	*Karl Rogers*
DHS	*Joe Jarzombek*
Managing Director	*Brent Baxter*
Publisher	*Kasey Thompson*
Managing Editor	*Drew Brown*
Associate Editor	*Chelene Fortier-Lozancich*
Article Coordinator	*Marek Steed*
Phone	(801) 775-5555
E-mail	stsc.customerservice@hill.af.mil
CrossTalk Online	www.stsc.hill.af.mil/crosstalk

CrossTalk, The Journal of Defense Software Engineering is co-sponsored by the Office of the Secretary of Defense (OSD) Acquisition, Technology and Logistics (AT&L); U.S. Navy (USN); U.S. Air Force (USAF); and the U.S. Department of Homeland Security (DHS). OSD (AT&L) co-sponsor: Software Engineering and System Assurance. USN co-sponsor: Naval Air Systems Command. USAF co-sponsor: Ogden-ALC 309 SMXG. DHS co-sponsor: National Cybersecurity Division in the National Protection and Programs Directorate.

The USAF Software Technology Support Center (STSC) is the publisher of CrossTalk, providing both editorial oversight and technical review of the journal. CrossTalk's mission is to encourage the engineering development of software to improve the reliability, sustainability, and responsiveness of our warfighting capability.

S T S C

***Subscriptions**:* Send correspondence concerning subscriptions and changes of address to the following address. You may e-mail us or use the form on p. 15.

517 SMXS/MXDEA
6022 Fir AVE
BLDG 1238
Hill AFB, UT 84056-5820

Article Submissions: We welcome articles of interest to the defense software community. Articles must be approved by the CrossTalk editorial board prior to publication. Please follow the Author Guidelines, available at <www.stsc.hill.af.mil/crosstalk/xtlkguid.pdf>. CrossTalk does not pay for submissions. Published articles remain the property of the authors and may be submitted to other publications. Security agency releases, clearances, and public affairs office approvals are the sole responsibility of the author and their organizations.

Reprints: Permission to reprint or post articles must be requested from the author or the copyright holder and coordinated with CrossTalk.

Trademarks and Endorsements: This Department of Defense (DoD) journal is an authorized publication for members of the DoD. Contents of CrossTalk are not necessarily the official views of, or endorsed by, the U.S. government, the DoD, the co-sponsors, or the STSC. All product names referenced in this issue are trademarks of their companies.

CrossTalk *Online Services:* See <www.stsc.hill.af.mil/crosstalk>, call (801) 777-0857 or e-mail <stsc.webmaster@hill.af.mil>.

Back Issues Available: Please phone or e-mail us to see if back issues are available free of charge.

When Tomorrow Becomes Today

As a child, I watched *The Jetsons*; it was a great show that I thoroughly enjoyed, but it led me to picture a 21st century where we would all be teleporting or driving personal spacecrafts to work. Likewise, my envisioned work environment included robots, mobile phones, and automated food mechanisms arriving at my desk at timely intervals throughout the day to provide hot and delicious snacks—all of this located within my organization where we manufactured fabulous cosmic products.

CrossTalk
would like to thank
309 SMXG for
sponsoring
this issue.

Looking back, if you trade my Toyota 4Runner for the spacecraft, my imagination was amazingly accurate. Allow me to compare my anticipated workplace with reality: Currently, my organization is heavily involved in robotics for use in various arenas; my cell phone can connect to anywhere in the world and can tell me where in the world I am; we produce software for use in all five levels of the Earth's atmosphere and outer space; and, for a few coins, I can eat food served to me from a vending machine—all of these are great advancements. Okay, the vending machine is a bit of a stretch, as at-work food delivery, or the quality of the snacks, hasn't evolved much. I guess we still have frontiers to be explored—at least gastronomically, if not astronomically.

The November/December issue of CrossTalk, themed *21st Century Defense*, explores slightly different advancements specific to the software defense industry. The software battlefront now includes laptops, desktops, servers, PDAs, cell phones, personal identification cards, and even a soldier's clothing. Each of these devices are utilized in our defense of the nation, as well as used against us by cyberattackers. Similarly, developing nations are advancing their technology at a more rapid pace than ever before. Electronic warfare (attack, support, and protection), drones, artificial intelligence, space platforms, miniature weaponry, and directed energy are all part of the new strategies planned in the defense of nations. Many of these weapons are nonlethal, but not all; many are aimed at rendering defense forces powerless by destroying software and systems before they can serve their purpose. The need to progress in our defense strategies and capabilities has never been greater, and this issue of CrossTalk presents several ideas to forward the cause.

We begin with *The Combat-Wireless Health Monitoring System* by MAJ Phillip G. Burns, who shares advances in identifying and monitoring a soldier's health and assessing injuries during combat, in turn speeding traumatic care and saving lives. Next, Susan Chandler and Jerrod Loyless' *PKI: The DoD's Critical Supporting Infrastructure for Information Assurance* (IA) explores the effective use of public key cryptography and how the Air Force is employing this technology to improve IA. In our final themed article, Summer Olmstead and Dr. Ambareen Siraj discuss the definition, history, laws, and defense methodologies of the new battlefront in *Cyberterrorism: The Threat of Virtual Warfare*.

Also in this issue, Anthony David Scott, Michael Malloy, Peter Clay, and Mark Masone's article—*Certification and Accreditation of SOA Implementations: Programmatic Rules for the DoD*—provides some interesting and valuable guidance for those faced with rapidly changing requirements on an SOA project. Finally, don't miss Jim O'Brien's *Preparing for an Internal Assessment Interview*, which offers practical insights regarding the nature of assessors and assists organizations in successfully participating in and surviving their next assessment.

It is our hope that this issue of CrossTalk will set the reader's mind in motion, stimulating new thoughts in regard to the future of software defense. There is no doubt that together, with the collective ideas and innovation of today, we will continue to be safe and secure well into the 22nd century.

Karl Rogers

Karl Rogers
Director, 309th Software Maintenance Group
Co-Sponsor

The Combat-Wireless Health Monitoring System

MAJ Phillip G. Burns
U.S. Army

The proposed combat-wireless health monitoring system (C-WHMS) allows for the seamless monitoring of a unit's medical health during combat operations, facilitating rapid injury identification and treatment. The C-WHMS quickly identifies soldiers who may have sustained traumatic injuries and whose lives may be saved by attending to them during the so-called "golden hour," as well as provides historical data to improve re-deployment and post-deployment health assessments.

Soldiers deserve the best medical care technology has to offer and should be the direct beneficiaries of technological advancements in trauma care. Such advancements include a comprehensive battlefield recording medical system, which is known as the Medical Communications for Combat Casualty Care (MC4).

The normal flow of events involves casualty identification by self-aid, buddy aid, or combat lifesaver. Once the casualty is identified, the combat medic provides tactical trauma care using appropriate medical equipment and supplies. In the past, the combat medic recorded medical care given to the casualty on a DD Form 1380 (Field Medical Card). In recent years, however, combat medics have used the MC4 system to record medical care given. The MC4 system is supported by a suite of applications that are included in the Defense Health Management Information System line of products. The MC4 has a store-and-forward capability, sending patient information forward when connectivity is available. Once the casualty is triaged with pertinent patient information captured on the MC4 system, the casualty is transported either to a battalion aid station or major treatment facility, as required.

As of today, the MC4 system has recorded more than 10 million electronic patient encounters using the MC4 system [1]. This technology, however, does not dynamically track injured soldiers at the point of injury. Research is underway to do just that by providing combat medics a means to remotely monitor casualties. One such technology is the Warfighter Physiological Status Monitor (WPSM). The WPSM will provide commanders and medics with the ability to actively monitor vital signs, core temperatures, and skin temperatures. Based upon acoustic measurements, ballistic impact detection will be monitored by the WPSM [2]. Researchers successfully tested the WPSM during a WMD exercise, remotely measuring vital signs and core temperatures of test subjects donned in chemical protective suits [3]. This research did not monitor concussions sustained by casualties.

This article proposes the development of a new C-WHMS as an alternative to the WPSM. The C-WHMS enhances the diagnostic capabilities of combat medics. The C-WHMS has yet to be built, but the reference technology is currently available. This article serves as a blueprint for combining technology into a single system.

> **"Without replacing the assessment or decision-making responsibilities of unit leadership and medical staff ... the C-WHMS will allow the combat medic to perform real-time monitoring of the unit's medical readiness during combat operations ..."**

Without replacing the assessment or decision-making responsibilities of unit leadership and medical staff, the role of the C-WHMS will allow the combat medic to perform real-time monitoring of the unit's medical readiness during combat operations, aiding the rapid identification of soldiers who may have sustained traumatic injuries. Telemedicine is a component of the C-WHMS, and allows the combat medic to communicate directly with a doctor over a video-conferencing system.

The proposed C-WHMS also includes a Military Smart Shirt that monitors soldiers' vital signs as well as pinpoints entrance and exit wounds. The C-WHMS allows combat medics to make a more accurate medical assessment of a traumatic injury as well as the level of shock the soldier may be experiencing. The C-WHMS includes a concussion monitoring system embedded within the Advanced Combat Helmet (ACH), which measures concussions sustained during the execution of combat operations. The components of the C-WHMS are discussed in this article, as well as the logical flow of responses to sensed data by the C-WHMS and the handling of alert messages emanating from the C-WHMS.

Before discussing the C-WHMS, a quick overview of Bluetooth is in order since it is an essential part of the C-WHMS.

Bluetooth Overview

Bluetooth networks (piconet) are generally comprised of seven slave nodes and one Master Node. If the Bluetooth is a Class I device, then the maximum communication distance is 100 meters in ideal conditions.

Bluetooth versions, prior to Bluetooth Version 2.1 + Enhanced Data Rate (EDR), communicate with their Master Nodes through a three-staged process: inquiry procedure, paging procedure, and established connection. Previous versions also supported the ability to avoid collisions with other slave nodes vying for the Master Node's attention via a back-off algorithm. According to researchers, this peer discovery and connection process led to a latency period not conducive to health care. They propose using Bluetooth Version 2.1 + EDR [4].

Researchers also argue that paging procedures—the main cause of connection latency—are not needed in Version

2.1; thus, the previous Bluetooth versions' three-staged connection procedure is collapsed into two stages: inquiry procedure and data delivery. Version 2.1 provides extended inquiry response, allowing 240 bytes of data transferred, along with the slave node's inquiry procedure [5].

Through simple secure pairing, researchers indicate that Version 2.1 can use public and private key pairing. This allows limited protection against passive eavesdropping and *man-in-the-middle* attacks [5]. With 79 possible channels and a frequency hopping rate of 1,600 hops per second, security is enhanced with Version 2.1.

To validate this level of security, testing in an electronic monitoring environment that replicates the battlefield environment is needed. Various components of the C-WHMS are based upon technologies geared to support the civilian sector. Power emissions of the Bluetooth device may need to be reduced to present a smaller footprint and target.

Finally, an election process is needed to elect Master Nodes when the primary Master Nodes are not available due to power failure or when out of communication range. In this article, the slave node is referred to as the Soldier's Local Server (SLS). The Master Node, however, retains its designation.

Components of the C-WHMS

The Military Smart Shirt

The Military Smart Shirt concept is based upon research and development of a smart shirt prototype by Georgia Tech in 1996. Initially funded by the Defense Advanced Research Projects Agency through the Department of the Navy, the smart shirt uses optical fibers to detect bullet and shrapnel wounds, using special interconnected sensors to monitor the body's vital signs during combat conditions. The smart shirt provides, for the first time, a systematic and personalized way of monitoring soldiers' vital signs—such as heart rate, electrical activity in the heart, body temperature, and pulse oximetry (SpO_2)—in an unobtrusive manner [6]. According to the researchers:

> Just as special-purpose chips and processors can be plugged into a computer motherboard to obtain the desired information processing capability (e.g., high-end graphics), the chosen motherboard paradigm provides an extremely versatile framework for the incorporation of sensing, monitoring, and information processing devices. [7]

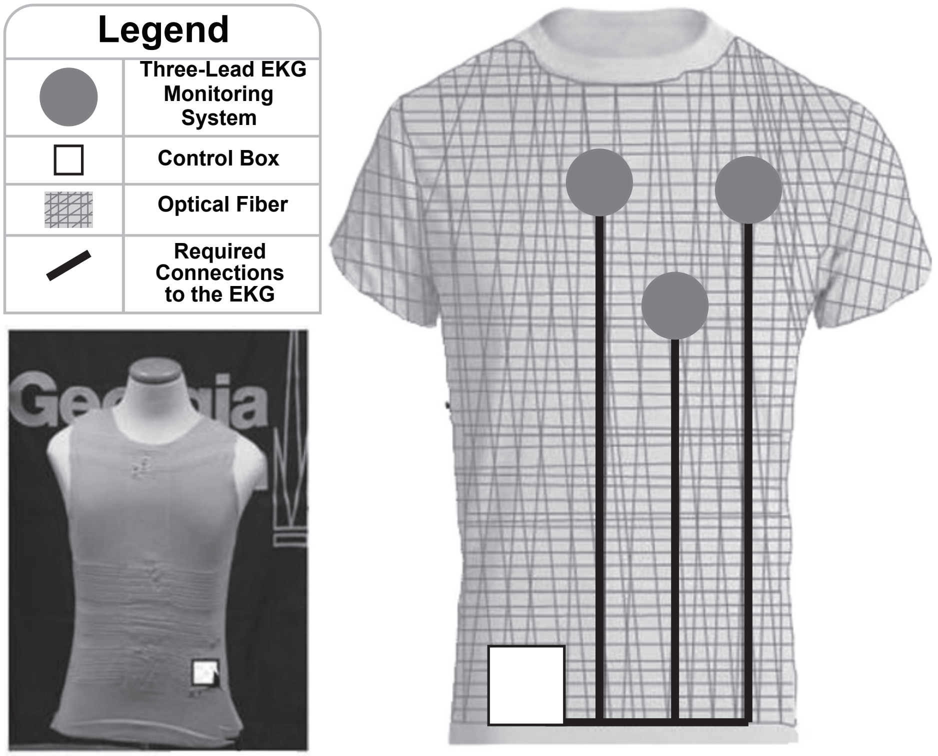

Legend
●
Three-Lead EKG Monitoring System
□
Control Box
▨
Optical Fiber
Required Connections to the EKG
Georgia

Figure 1: *Military Smart Shirt*

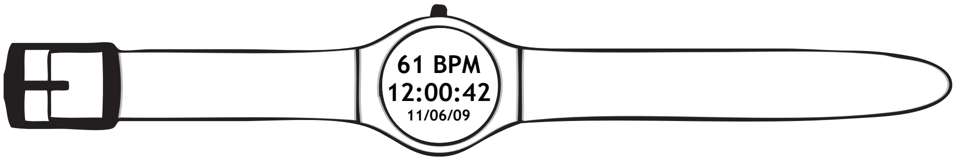
Several versions of the smart shirt have been produced. With each succeeding version, the garment has been continually enhanced from all perspectives: functionality, capability, comfort, ease of use, and aesthetics. VivoMetrics provides a commercially developed example of another approach to monitoring vital signs with the LifeShirt [8].

Based upon Georgia Tech's initial research, Figure 1 illustrates a proposed Military Smart Shirt, consisting of a three-lead electrocardiogram (EKG) monitoring system, optical fibers, and a control box. Since the Military Smart Shirt can monitor multiple vital signs, it doesn't need to be restricted to taking an EKG. For instance, SpO_2 is very useful for seeing if there is enough oxygen in the blood (and going to the brain). The three-lead EKG monitoring system periodically performs a check of the soldier's vital signs. The control box receives vital signs from the three-lead EKG monitoring system, then forwards sensed data to the SLS—a wearable watch (as shown in Figure 2).

In addition to the three-lead EKG monitoring system, the Military Smart Shirt consists of optical fibers. These fibers are interconnected with sensors that gauge whether or not they have been severed due to a foreign object, registering the exact location of an entrance or exit wound. After the penetration of the Military Smart Shirt, continuous monitoring of the soldier's vital signs is required. The control box monitors the system health of the shirt and records data from optical fibers and the three-lead EKG monitoring system.

In [9], the authors illustrate how data transfer paths for the Military Smart Shirt must be programmed to ensure effective integration and communication between the control box and sensors via optical fibers. The arrangement of the control box is critical in creating an architecture that is wearable, washable, and flexible, while serving as a motherboard that can fulfill stated requirements. Power consid-

Figure 2: *Soldier's Local Server*



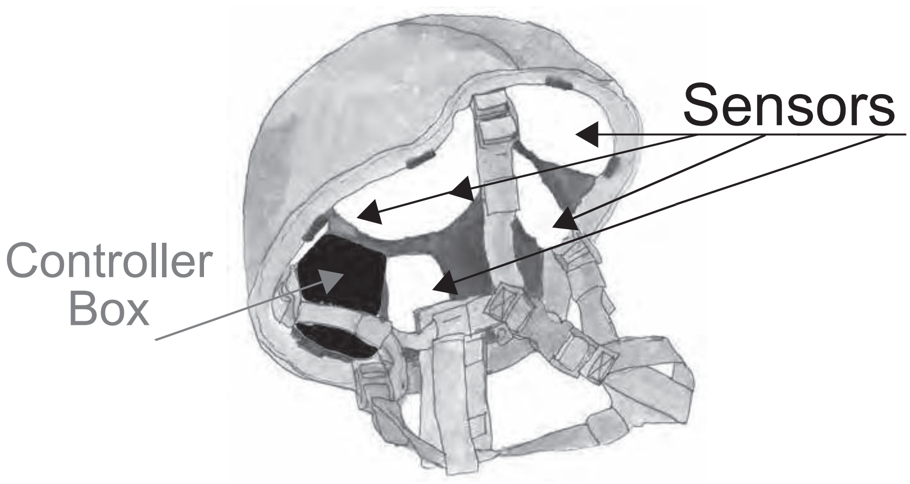


Figure 3: *ACH Concussion Monitoring System with Sensors*

erations are an important consideration as well. Ongoing missions will require a means to repower or replace power-depleted Military Smart Shirts.

The ACH Concussion Monitoring System

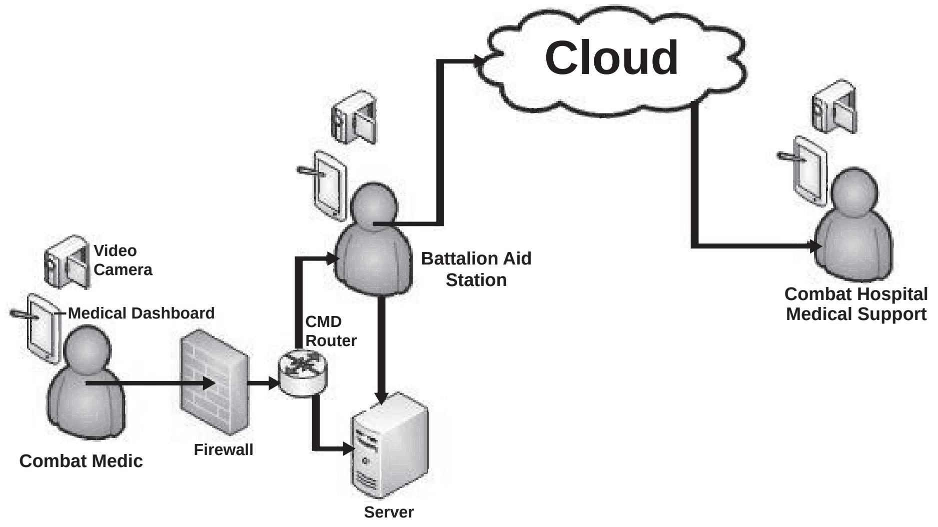
The concussion monitoring system is the second component of the C-WHMS, as embedded in the ACH. Concussions sustained by soldiers are a major concern of military leadership. The goal is to quickly and accurately assess cases of suspected brain trauma injuries.

Currently, the Military Acute Concussion Evaluation (MACE) exam is used extensively by military medical personnel to confirm the diagnosis of a mild or severe case of brain trauma. As a tool, MACE is based upon the soldier's medical history of previous brain trauma injuries and uses standardized tests to gauge the impact of the brain injury on memory and concentration [10]. MACE lacks electronic records of actual brain trauma sustained during combat operations. The proposed concussion monitoring system provides an automated means to electronically record brain trauma injury, providing real-time notification to combat medics; it augments—but does not replace—MACE.

There are two options for automating the means of electronically recording traumatic brain injuries. The first option is based upon Riddell's product: Riddell Revolution IQ HITS. This system is a football helmet capable of storing up to 100 impacts. This equipment sends impact data to wireless monitoring systems located on the sidelines [11].

Figure 3 shows that an ACH can be retrofitted with sensors that serve dual purposes: as cushions and impact sensors. The control box would be located behind the rear stabilizing pad and would monitor data from impact sensors. As soldiers may potentially drop their ACH while not wearing it, false positives can be reduced by requiring all sensors to have positive contact with the wearer's head for the system to function.

Figure 4: *Combat Medical Dashboard System*



If a severe impact is sensed, then the data is stored in the control box and is forwarded to the SLS. An outtake of the soldier's vital signs is taken to determine the medical status of the soldier and whether or not the soldier is in the beginning stages of shock. The control box can store 100 counts of impact that exceed threshold levels as well as associated vital signs, forwarding data to the SLS if a registered impact exceeds pre-established thresholds.

The second option is the Helmet Sensor as tested and fielded by the Project Manager Soldier Survivability Team at Fort Hood, Texas. Testing demonstrates that a one-ounce monitor can track the concussions and overpressure that a soldier experiences during a blast event. The sensor system can easily record a month's worth of data, downloading data via a USB port to a computer [12]. This is the more promising and viable of the two options. Adapting this technology to wirelessly forward traumatic brain injury information to the SLS could prove extremely beneficial.

The SLS

The SLS is the third component and is a member node of the Bluetooth network, communicating with its controlling Master Node. This Master Node communicates with the combat medic's dashboard system (CMDS). Communication with the Master Node is not soldier-initiated, and is predetermined prior to the start of a mission.

There are many commercially available biometric watches that support Bluetooth technology. Such watches have the ability to monitor the wearer's heart rate. Such technologies demonstrate the feasibility of Bluetooth transmission of GPS signals to an array of devices, such as PDAs and smart phones, for the purpose of navigation.

In August 2000, a team of IBM researchers began the task of building a wearable server, designed as a watch. They developed a Bluetooth-enabled prototype that runs on Linux and X11 [13]. This system has the potential to run the services required to monitor the Military Smart Shirt and the concussion monitoring system, as it is able to store and transmit vital signs that cross pre-established thresholds. In addition, it is recommended to add to the wearable server the ability to conduct heart rate monitoring in the event the shirt becomes inoperable.

The SLS compares received vital signs

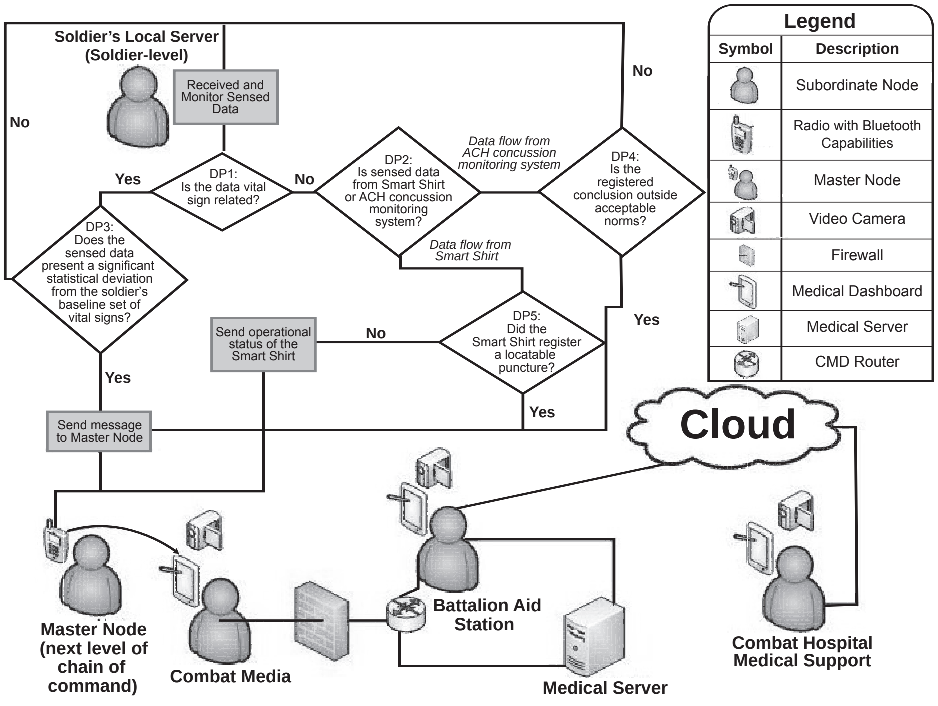

Soldier's Local Server
(Soldier-level)
Received and Monitor Sensed Data
No
No
DP1: Is the data vital sign related?
Yes
No
DP2: Is sensed data from Smart Shirt or ACH concussion monitoring system?
Data flow from ACH concussion monitoring system
DP4: Is the registered conclusion outside acceptable norms?
Data flow from Smart Shirt
DP3: Does the sensed data present a significant statistical deviation from the soldier's baseline set of vital signs?
Send operational status of the Smart Shirt
No
DP5: Did the Smart Shirt register a locatable puncture?
Yes
Yes
Yes
Send message to Master Node
Cloud
Legend
Symbol
Description
Subordinate Node
Radio with Bluetooth Capabilities
Master Node
Video Camera
Firewall
Medical Dashboard
Medical Server
CMD Router
Master Node (next level of chain of command)
Combat Media
Battalion Aid Station
Medical Server
Combat Hospital Medical Support

Figure 5: *Logical Flow of the C-WHMS*

against stored baseline averages. This is important because missions differ, requiring soldiers to put forth varying levels of physical exertion. Upon conclusion of the mission, vital sign values are transmitted to the medical server located at the battalion aid station via the Master Node and the CMDS. This data is relevant for both re-deployment and post-deployment health assessment as the data is included in the soldier's electronic medical record (EMR), facilitating communication between supporting healthcare professionals.

The Master Node

The Master Node is the fourth component, Bluetooth-enabled to the Single Channel Ground and Airborne Radio System (SINCGARS), or a squad radio variant. This radio is operated by unit leadership. The authors of [14] indicate a need for the development of a communication link between a PDA and a SINCGARS radio, outlining functional and nonfunctional requirements to accomplish this capability [10]. Linking the SINCGARS radio with the Master Node and the CMDS can possibly augment communication distances.

The Master Node is the controlling member of a seven-member piconet. Since infantry squads are divided into two five-man teams, the seven-member is ideal to support team-level maneuvers, as well as a single High Mobility Multipurpose Wheeled Vehicle crew. This Master Node relays messages from its piconet to the CMDS; however, communication is not initiated by the squad leader. This allows vital medical information to be forwarded to the combat medic without impacting the overall mission. This seamless transmission of medical data does not exempt leaders from their responsibility of checking on the welfare of their subordinate soldiers as the mission dictates. It does, however, facilitate the rapid identification of soldiers who may have become casualties, requiring immediate evacuation.

The CMDS

The last component, the CMDS, is based upon the principles of Business Activity Monitoring. Figure 4 illustrates the dashboard as adapted to the combat medic's needs. The CMDS provides an iconic view of the unit's medical readiness. The goal is to ultimately interface the CMDS with the Army's MC4.

There are four sets of icons at the heart of this notification; they show: vital signs, any optical fiber severing, ACH impact counts that exceed pre-established limits, and system diagnostics. Each icon has a number in the center representing the number of alert messages. As the combat medic receives an alert message on their CMDS, the combat medic has the ability to *drill-down*, reviewing individual alert messages (as needed) by simply double-clicking the icon.

The combat medic's prioritization of medical needs and medical resources is based upon a green, amber, and red color-coded scheme. A green icon indicates normal operation; an amber icon indicates caution; and a red icon scheme indicates a potential emergency situation that can lead to a loss of limb or life if left unchecked. The handling of alert messages is discussed later in this article.

The proposed CMDS has the capability to communicate with a doctor via video-conference. Telemedicine extends beyond diagnostic capabilities and tools already available to the combat medic. Telemedicine supports the combat medic as he or she stabilizes a soldier under the direct supervision of a doctor prior to transport, even though time and distance limit the doctor's ability to be physically present. In these critical cases, the CMDS allows combat medics to consult directly with a doctor or physician's assistant via an attached video camera, showing the extent of injuries. The CMDS supports the storage of the soldier's EMR as synchronized with the medical server. This allows doctors to view the same EMR data as the combat medic has on the CMDS screen.

Telemedicine allows the combat medic to continue medical support while in transit to the battalion aid station or combat hospital. Also, the battalion aid station is equipped with a variant of the CMDS, allowing consultation over the Internet with other healthcare professionals (as needed). The next section demonstrates the logical flow of the C-WHMS in action, relating the five components of the C-WHMS.

C-WHMS: How it Works

Figure 5 presents a logical flow of responses by the sensors to the operational environment, enhancing the medical status reporting of units conducting combat patrols or convoy operations. Figure 5 starts with the SLS. The SLS represents the soldier and the soldier's network of sensors, including the ACH concussion monitoring system and Military Smart Shirt. Embedded within the squad communication system, a Bluetooth-enabled device monitors the medical readiness of the soldier.

If the device detects an abnormality in sensed data, then that data is routed along five decision points (DPs). The first decision point, DP1, provides the first essential filtering function. DP1 asks if the abnormality of sensed data is vital sign-related only, related to a concussion sustained by the casualty, or a puncture of the Military Smart Shirt, indicating the potential entrance of a bullet or shrapnel fragment.

If the answer is *yes*, then sensed data is routed to DP3, which asks: Does the sensed data represent a statistical deviation of the soldier's baseline of stored vital signs value? If the sensed data is not a statistical deviation from the norm, then the monitoring system continues its passive monitoring. If the sensed data presents a statistical deviation from the norm, then an alert message is routed from the Master Node to the combat medic.

If the answer to DP1 is *no*, then DP2 is queried: Is the sensed data coming from the Military Smart Shirt or the ACH concussion monitoring system? If the answer to DP2's query is related to the ACH concussion monitoring system, then DP4 checks to see whether or not a concussion is registered by the system. If a concussion is sensed, an alert message is sent from the SLS through the Master Node to the combat medic.

If the answer to DP2's query is Military Smart Shirt-related, then DP5 checks to see if it has registered a locatable puncture. The exact location of the puncture is essential. At this point, vital signs are measured regularly in order to determine whether or not the soldier is in shock. As this shock is a significant event, a high-alert message is immediately forwarded to the combat medic. If the exact location of the puncture cannot be determined, a check of the Military Smart Shirt's operational status is performed. If it is not functional, the combat medic receives a low-level alert message, and the soldier's vital signs are monitored as a precaution. The combat medic monitors the operational situation, contacting the soldier as the mission dictates.

At the conclusion of the military operation, the Master Node (as directed by the patrol or convoy commander) conducts a network call, retrieving data stored from all members of its piconet. This data is stored in the medical server and is accessible and used during redeployment and post-deployment health assessments.

Handling of Alert Messages

Alert messages are handled in the following manner: Icons representing vital signs, the severing of optical fibers, and impact counts display a color code with a number representing the total number of associated alert messages. Alert messages are forwarded from the SLS through the Master Node to the CMDS.

Red alert messages are forwarded automatically to the unit's battalion aid station or supporting combat hospital. This allows the next level of medical care to prepare for a potential influx of casualties. Also, the soldier's EMR is forwarded to the next level of medical care: thorough review of the soldier's EMR (for allergies to any medications) and medical history (for mitigation of any potential complications). Red alert messages are of highest priority. Unit leadership is notified immediately of this type of message because it indicates a high possibility that a loss of limb or life may result if left unchecked.

> ***"Red alert messages are forwarded automatically to the unit's battalion aid station or supporting combat hospital. This allows the next level of medical care to prepare for a potential influx in casualties."***

Alert messages contain sensed data as well as the GPS location of the injured soldier. If the sensed data pertains to the severing of optical fibers, the exact location is sent along with the alert message in order to help the combat medic accurately identify entrance and exit wounds (as needed). Vital signs are included in all alert messages as this allows the combat medic to monitor the soldier for shock.

Amber-colored alert messages are forwarded to the next level of medical care for information purposes only. This allows the battalion aid station to track changes as they occur, pre-position medical supplies as the condition deteriorates, and brief the battalion commander on up-to-the-minute medical readiness information. Amber alert messages are of medium concern, handled locally when the mission permits. Green alert messages are a low priority and handled locally when the mission permits. They are not automatically forwarded to the next level of medical care unless the combat medic decides to send the data.

Conclusion

This article shows it is demonstrably feasible to develop the C-WHMS with available wireless technologies. Tailoring such technology to meet the needs of the military could yield benefits in the arena of military healthcare and battlefield triage, potentially saving lives. Off-the-shelf software, specific to the medical community, should be evaluated in greater detail, modifying it as necessary to adapt to military uses for medical care.◆

Acknowledgement

The author wishes to acknowledge Dr. Sundaresan Jayaraman for his mentorship and contribution to the Military Smart Shirt section. Dr. Jayaraman is a professor at the School of Polymer, Textile and Fiber Engineering at Georgia Tech.

References

1. Steen, Ray. "Army Program Celebrates 10 Years of Delivering Battlefield Medical Information to War Fighters: MC4 Announces New Strategic Plan." MC4. 18 May 2009 <www.mc4.army.mil/pressreleases/090518_MC4_10years_StrategicPlan.asp>.
2. Military Operational Medicine Research Program. "WPSM Initial Capability." 2008 <https://www.momrp.org/pm3.html>.
3. U.S. Army Soldier Systems Center – Natick (MA). "Researchers Test Warfighter Physiological Status Monitor." 27 July 2007 <www.army.mil/-news/2007/07/26/4157-researchers-test-warfighter-physiological-status-monitor>.
4. U.S. Army Soldier Systems Center – Natick (MA). "USARIEM Researchers Test WPSM Capabilities During Training Exercise." SSC-Natick Press Release, Public Affairs Office. 23 July 2007 <www.natick.army.mil/about/pao/2007/07-23.htm>.
5. Lee, Seung-Hoon, et al. *Bluetooth 2.1-Based Emergency Data Delivery System in HealthNet.* Proc. of the Wireless Communications and Networking Conference. Las Vegas: 31 Mar.-3 Apr. 2008 <www.cs.ucla.edu/~shlee/papers/eir.ppt>.
6. Park, Sungmee, et. al. "The Wearable Motherboard: An Information Infrastructure or Sensate Liner for Medical Applications." *Studies in Health Technology and Informatics* 62 (1999): 252-258.
7. Gopalsamy, Chandramohan, et al.

Software Defense Application

This article demonstrates to the DoD software community how an emerging field—pervasive healthcare—can be applied to a military setting. A central feature of pervasive healthcare is ubiquitous computing. Ubiquitous computing is the seamless and unobtrusive integration of information systems into everyday objects. The proposed C-WHMS illustrates this concept—where the return on investment is not so much monetary as it is the preservation of human life. Since the C-WHMS is a concept for now, the ROI is not based upon monetary value.

"The Wearable Motherboard: The First Generation of Adaptive and Responsive Textile Structures for Medical Applications." *Journal of Virtual Reality* 14 (1999): 152-168.

8. VivoMetrics. "About LifeShirt." <www.vivometrics.com/lifeshirt>.
9. Park, Sungmee, Kenneth Mackenzie, and Dr. Sundaresan Jayaraman. *The Wearable Motherboard: A Framework for Personalized Mobile Information Processing*. Proc. of the 39th Design Automation Conference. New Orleans: 10-14 June 2002.
10. "Military Acute Concussion Evaluation Offers Quick Diagnosis After Head Injury." *MEDCOM Now* 2.2. 1 Feb. 2008 <www.amedd.army.mil/medcom/MEDCOM _Now_20080201-vol2-issue2.pdf>.
11. Nilay, Patel. *Engadget*. "Riddell Starts Shipping Concussion-Monitoring Football Helmets." 18 Dec. 2007 <www.engadget.com/2007/12/18/riddell-starts-shipping-concussion-monitoring-football-helmets>.
12. Myles, LTC Robert. "Helmet Sensors Fielding, Fort Hood." Online video. Program Executive Office Soldier. <https://peosoldier.army.mil/video/fthood.htm>.
13. Narayanaswami, Chandra. "IBM's Linux Watch: The Challenge of Miniaturization." 25 Sept. 2002 <www.eecs.utoledo.edu/~ewing/ieee/meetings/notices/25sep2002.pdf>.
14. Alford, Kenneth L., et al. "Platform Independent Tactical Data Entry Devices." CrossTalk Aug. 2002 <www.stsc.hill.af.mil/crosstalk/2002/08/alford.html>.

About the Author

MAJ Phillip G. Burns currently attends Georgia State University as a graduate student, pursuing a master's degree in computer information systems. He serves as the Graduate Business Association's vice president of technology. In 2007, Burns graduated from the Information Systems Officer course at the U.S. Army's School of Technology at Fort Gordon, Georgia.

10810 Glenbarr DR
Johns Creek, GA 30097
Phone: (678) 548-9927
E-mail: phillip.g.burns@us.army.mil

PKI: The DoD’s Critical Supporting Infrastructure for Information Assurance

Susan Chandler
Booz Allen Hamilton

Jerrod Loyless
General Dynamics C4 Systems

The DoD’s Public Key Infrastructure (PKI)[1] provides general-purpose PKI services to a broad range of applications through effective use of public key cryptography. This article presents a quick overview of the Defense-in-Depth strategy, briefly explains key PKI elements and security mechanisms, and addresses how the Air Force is employing this technology to improve information assurance (IA).

As the Internet rapidly expanded in the ’90s, so did the DoD’s usage of the Web to provide global support to the warfighter. The Internet, being an open environment, was not secure enough to conduct mission-critical, unclassified transactions. Therefore, to fully benefit from this new medium, a more secure capability had to be put into place. Specifically, Internet-based transactions would need to provide a reliable means to: conduct private communications between parties on the public Internet, verify a party’s identity over the Internet, replace handwritten signatures, and ensure that data is not altered during transmission.

Today, adversaries, in their current quest to subvert DoD capabilities by debilitating critical information assets, are coming from all directions. Terrorists, hackers, unfriendly nation states, and various types of criminal elements—motivated by the acquisition of top-secret intelligence, financial gain, intellectual property theft, denial of service, or simply pride in exploiting a notable target—are routinely attacking DoD networks. Their methods range from passively monitoring communications to social engineering to full-blown active network attacks with viruses and other malicious means.

Consequently IA, at least in DoD terms, is achieved when information and information systems are protected against such attacks through the application of critical security services such as availability, integrity, authentication, confidentiality, and non-repudiation.

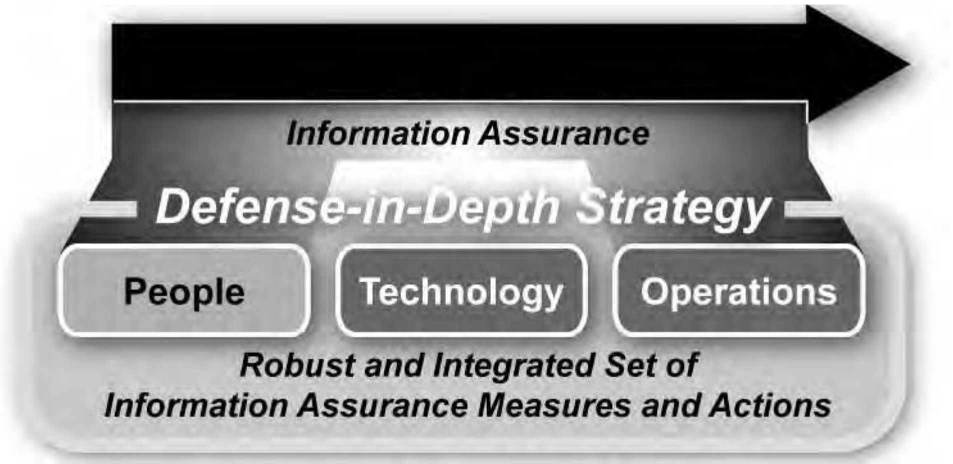
Defense-in-Depth Strategy: A Quick Overview

The DoD’s Defense-in-Depth strategy is a practical method for achieving IA in today’s highly networked environments [1]. It uses a *best practices* approach that relies on intelligent applications of existing techniques and technologies. The strategy recommends a balance between the protection capability and the cost, performance, and operational considerations of the overall DoD mission. Comprised of a robust and integrated set of IA measures, the strategy hinges on the balanced focus of three primary elements: people, technology, and operations (see Figure 1).

The people element encompasses establishing, applying, and enforcing applicable policies and procedures, assigning roles and responsibilities, committing resources, training critical personnel (e.g., users and system administrators), and requiring personal accountability [1]. This includes establishing physical security and personnel security measures to control and monitor access to facilities and critical elements of the IT environment such as networks and systems.

A wide range of technologies are available that provide IA services and intrusion detection. To ensure the right technologies are procured and deployed, the technology element focuses on the establishment of effective policies and processes for technology acquisition and is grounded on two primary IA principles: defense in multiple places and having layered defenses.

Figure 1: *Defense-in-Depth Strategy*


Information Assurance
Defense-in-Depth Strategy
People
Technology
Operations
Robust and Integrated Set of
Information Assurance Measures and Actions

Given that adversaries can attack from multiple points using either insiders or outsiders, protection mechanisms at multiple locations are in place to facilitate resistance to all classes of attacks [1]. Focus areas (shown in Figure 2) include defending:

- **Networks and Infrastructure.** Protecting the local and wide area communications networks and providing confidentiality and integrity protection for data transmitted over these networks.
- **Enclave Boundaries.** Deploying firewalls and intrusion detection to resist active attacks.
- **The Computing Environment.** Providing access controls on hosts and servers to resist insider, close-in, and distribution attacks.

The best available IA products can still have inherent weaknesses; therefore, multiple and layered defense mechanisms are deployed as unique barriers between the adversary and its target to deter exploitation of possible vulnerabilities, increase the probability of detection, and reduce the chances of successful penetration [1]. Focus areas include multiple supporting infrastructures:

- Deployment of nested firewalls at outer and inner network boundaries.
- Specification of security robustness of each IA component as a function of the value of what it’s protecting.
- Deployment of robust key management infrastructures and PKIs that support all IA technologies and are highly resistant to attack.
- Deployment of methods to detect intrusions, analyze and correlate the results, and then react accordingly.

PKI as a Supporting Infrastructure

Now that the big picture is in place, it’s time to illustrate how the PKI and its foundational element of public key cryptography is a critical supporting infrastructure to the overall strategy. In its essence, public key cryptography provides three functions that help meet the needs of the Defense-in-Depth strategy: identity authentication, digital signatures, and public key encryption—all operating within a chain of trust[2].

Identity authentication establishes the validity of an entity's claimed identity and is used in making access-control decisions. The entity may be a user, a Web service, or a device.

A digital signature is an electronic code that can be attached to data. It identifies the signer of the data and associates the signer with the data being signed. Digital signatures verify that the signer is really the person or entity he or she claims to be, or be a part of, and that the signed data was not modified.

Public key encryption allows multiple users to efficiently exchange encrypted data. Public key encryption establishes a common encryption key over the network without giving away enough information for someone observing the transaction to deduce the key. Together, digital signatures and public key encryption allow two or more communicating parties to positively identify one another and keep their communications confidential [2].

Public key systems issue a pair of keys to each user: a private key, which the user does not disclose to anyone, and a public key, which is publicly advertised. A signer encrypts data using the recipient's public key, and the receiver decrypts it with their private key. Public keys are contained in data structures called certificates. Certificates contain a digital signature from an issuing authority and the user's identification, which binds the user's identity to their public key.

Several support services are required to use public key cryptography, including a means of issuing, distributing, and advertising keys and certificates; a way to verify certificate authenticity; and a process to revoke them. These services are provided by an integrated combination of equipment and administrators collectively known as the PKI.

One more component is required to implement public key cryptography: computer applications that support its use. The PKI provides a credential service for these applications. Applications are not directly part of the PKI, but public key-enabled applications improve access control by leveraging PKI-based identity authentication, and digital signatures on electronic forms automate many business processes that traditionally rely on the exchange of paper forms and handwritten signatures. Public key encryption provides confidentiality for sensitive, unclassified data over the non-secure IP Router Network (NIPRNet) and provides confidentiality for restricted groups on classified networks.

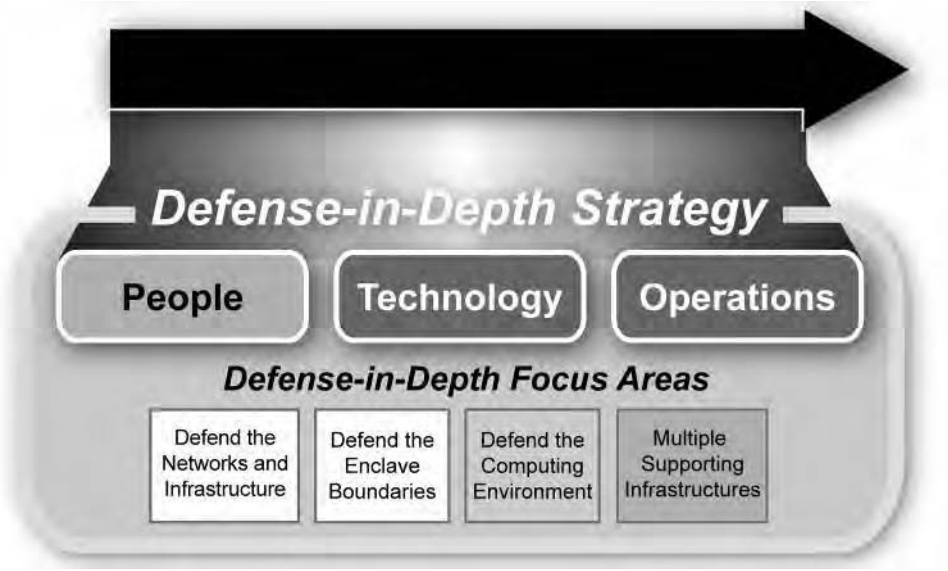

Defense-in-Depth Strategy
People
Technology
Operations
Defense-in-Depth Focus Areas
Defend the Networks and Infrastructure
Defend the Enclave Boundaries
Defend the Computing Environment
Multiple Supporting Infrastructures

Figure 2: *Defense-in-Depth Focus Areas*

Secret Key and Public Key Cryptography

To understand public key cryptography, it is useful to understand traditional *secret key cryptography*. Secret key cryptography is also known as *symmetric* key cryptography because the same key is used to encrypt and decrypt the data using the same algorithm in the same direction (Figure 3). Clear-text data (i.e., data in its original form) is transformed (encrypted) into cipher text, which is incomprehensible. The cipher text can only be decrypted, or transformed to the original clear text, by someone who has a copy of the encryption key. One can try to guess the key, but the objective of cryptography is to make guessing not feasible.

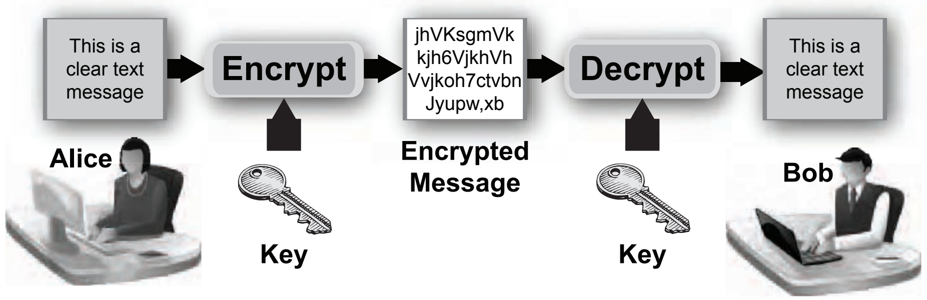
There are major challenges with using symmetric key cryptography, one of which is finding a secure way to provide keys to other parties so that secure communication between them is possible. In a small office, one can hand-carry keys to the other parties, but as the number of correspondents becomes larger and more geographically dispersed, this process soon becomes impractical.

A second major challenge is difficulties of scale. The secret key shared between two parties (e.g., Alice and Bob shown in Figure 3) must be different from the secret key shared between Alice and someone else; otherwise, the confidentiality of messages intended for Bob is compromised. Because the same is true for every user, this community could collectively hold millions of unique secret keys. As the community grows, the storage and maintenance of such large numbers of keys becomes unmanageable [2].

Public key cryptography is referred to as *asymmetric* cryptography because it uses two different keys: a public key and a private key (see Figure 4, page 13). One key is kept private[3], and the other is made public. For example, if Bob publishes his public key, anyone with access to his public key can encrypt a message to Bob. Since the public key cannot be used to decrypt the message, only Bob (who is the sole possessor of the corresponding private key) can decrypt the message.

Public key cryptography is more mathematically complex than secret key cryptography, therefore it is slower. To speed the process, public key cryptography passes a session, message, or bulk encryption key—which are secret keys used for subsequent encryption and decryption. In addition to

Figure 3: *Secret Key Cryptography*



providing confidentiality through encryption, public key cryptography is used for digital signatures[4] and identity authentication.

PKI Core Services

As the DoD becomes increasingly reliant on computer networking to achieve information superiority over adversaries, the core services provided by a PKI (i.e., authentication, integrity, confidentiality, and non-repudiation) become increasingly critical.

Identification and Authentication

Identification is defined as the process an information system uses to recognize an entity, while authentication is a security measure designed to establish the proper assurance level of a claimed identity [2]. A user's identity is authenticated as part of the certificate-issuance process. Identification and authentication are useful for granting authorization to information on a server via remote access, protecting network management from masqueraders (i.e., persons attempting to use counterfeit or stolen credentials and gaining physical access to a restricted area).

Data Integrity

Integrity is the assurance of non-alteration and it is this security service's job to detect unauthorized modification or destruction of information [2]. Digital signatures support data integrity verification. In contrast to handwritten signatures, verification of a digital signature relies on the authentication of the signer's identity and proves that the data remains unchanged.

Non-repudiation

Non-repudiation provides undeniable proof of a party's participation in a communication. The basic idea is that a user is cryptographically bound to a specific transaction in such a way that they cannot deny (repudiate) having conducted the transaction [2]. Activities such as command and control, official release of procurement documents, and travel reimbursement approvals are accompanied by legal requirements for non-repudiation. The DoD satisfies these legal requirements with PKI's digital signature capability.

Confidentiality

Confidentiality is the assurance of data privacy. It ensures that information is not disclosed to unauthorized persons, processes, or devices [2]. Various types of transactions—such as Web-based access, file transfers, network management, payment transactions and secure messaging—require confidentiality to protect sensitive unclassified message data against *eavesdropping*; that is, unauthorized persons or entities being able to gather information by actively or passively monitoring network traffic [3, 4, 5, 6].

Multiple Assurance Levels: Not All Information Is Created Equal

As a credential service, a PKI binds user and entity identities with digital certificates and associated public keys. The level of assurance of a public key certificate is an assertion by a Certification Authority of the degree of confidence a relying party may reasonably place in the binding of a user's public key (and thereby the private key) to the identity and privileges asserted in the certificate [7]. The processes and controls employed in PKI operations, the methods used to protect the users' private keys, and the strength of the cryptographic algorithms used, all serve a role in determining the PKI's assurance level.

> *"Not all information is created equal ... Some types of information are extremely valuable to an attacker, while others have almost no value. On the other hand, some information may be freely disclosed but would be disastrous if it was corrupted or destroyed."*

Not all information is created equal, however. Some types of information are extremely valuable to an attacker, while others have almost no value. On the other hand, some information may be freely disclosed but would be disastrous if it was corrupted or destroyed. Threats[5] vary based on the value of information and the networking environment in which it resides. And while a single solution—providing support to every application—would appear to be desirable, different legal, security, and national policy requirements for protecting the different categories of information (such as administrative, e-commerce, Mission Assurance Category I and II, etc.), necessitate the most cost-effective solution as one which supports multiple assurance levels.

In [7], the various levels of assurance for DoD's PKI are defined: *Medium, Medium 2048, Medium Hardware, Medium Hardware 2048, Personal Identity Verification (PIV) Authorization, PIV Authorization 2048*, and *High*. The applicability of the different assurance levels is determined by the value of the information being protected and the threat environment. *Medium* assurance levels are intended to protect applications handling medium-value information in a low-to medium-risk environment. The NIPRNet, where the majority of DoD business is conducted, is an example of a medium assurance environment.

PKI Security Mechanisms and Supporting Services

As mentioned previously, a PKI is a complex system of integrated components, mechanisms, and security services that work in concert to support the long-term integrity of application data. The following illustrates these underlying security mechanisms and their supporting services:

Security Mechanisms

Key Exchange

Key exchange is the process that communicating parties use to establish a common key for secure communications. There are several ways an originating party can obtain the receiving party's public key: from a directory, directly from the receiving party as part of an online key exchange protocol, or from a cache (if the originating party had some prior communication with the receiving party). Issuing Certification Authorities automatically post subscribers' public keys to the Global Directory Service[6], and in the Air Force, users also publish their own public keys to the Air Force Global Address List for easy access.

Digital Signatures

In the digital signature process (as illustrated in Figure 5), a hash algorithm (i.e., a message digest) is produced. The hash is encrypted using the signer's private key. After receiving the message, the recipient decrypts the hash using the signer's public key and compares it to a hash calculated from the received message. If the two are a match, the recipient knows that: a) the message was not changed from the time the signer applied the signature and b) the signer's private key was used; therefore, the message must have come from the signer [2].

Data Recovery

Data recovery is a security service that enables the originator to recover inaccessible data or permits an authorized third party to gain access to encrypted information. Legitimate reasons data recovery may be necessary are: a user obtains new PKI certificates and keys, and the original key that encrypted data is no longer available; the owner departs the DoD and leaves behind encrypted official data that needs to be accessed; and for legal or intelligence investigations.

Key Escrow and Key Recovery

Key escrow is the process of storing private encryption keys for the purpose of enabling data recovery. It automatically occurs during the certificate issuance process. Digital signature keys are not escrowed.

Key recovery is the process of obtaining a copy of an escrowed encryption key and delivering it to an authorized requester. Key recovery systems store a copy of a user's private encryption key in a secured database, allowing access by authorized personnel known as Key Recovery Agents (KRAs). KRAs are highly trusted personnel responsible for recovering archived certificates in very specific situations. The process of key recovery is protected by two-person integrity; keep in mind, however, that signature keys are not recoverable.

Supporting Services

Key Generation

Key generation generates the public-private key pair that enables public key cryptography functions. User keys are encrypted onto an authorized token (i.e., a smart card) or removable storage media (e.g., a CD). The DoD ID card, known as the Common Access Card (CAC), is a smart card and is the preferred token for PKI certificates and keys [8].

Certificate Generation and Revocation

Once the key pair is generated, associated certificates are generated by the issuing Certification Authority server. For users, the process of generating keys and issuing certificates is combined.

Certificate revocation is necessary when a certificate becomes invalid before its expiration date; there's reason to believe the private key associated with the certificate is compromised (e.g., the token is lost); a user no longer represents an organization; and when information in the certificate is no longer valid. Relying parties are notified that a user's certificate is revoked via certificate revocation lists (CRLs) published by the issuing Certification Authority.

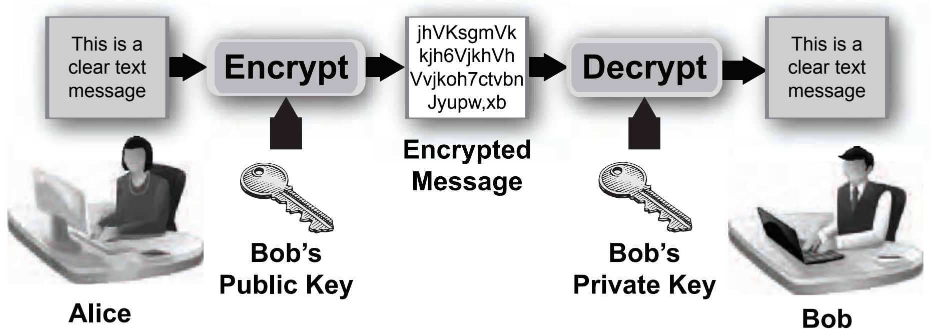

This is a clear text message
Encrypt
jhVKsgmVk kjh6VjkhVh Vvjkoh7ctvbn Jyupw,xb
Encrypted Message
Decrypt
This is a clear text message
Alice
Bob's Public Key
Bob's Private Key
Bob

Figure 4: *Public Key Cryptography*

Certificate Expiration, Updating, and Re-keying

Public-private key pairs have finite lifetimes to protect against key compromise; therefore, associated certificates also include a validity period. Users must obtain new certificates in a timely fashion to prevent any disruption in service. Certificate re-key provides for replacement prior to a certificate's expiration. The process for updating or re-keying a certificate is similar to the process for initially issuing the certificate: The registration process is repeated to ensure the reason for having a certificate remains valid, and the user's identity is authenticated.

Archives

Archives provide a long-term repository for storing information. Even though the lifetime of a Certification Authority is relatively short, it may be necessary to verify signatures on old documents at a later date. To support this need, the PKI archive service stores user registration information, certificates, and CRLs issued by the Certification Authority.

Common Access Cards

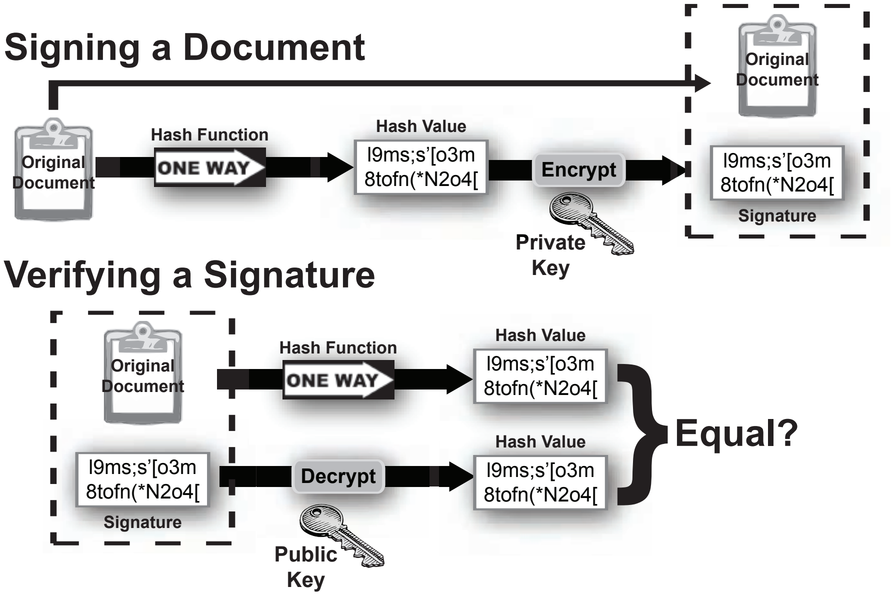
First and foremost, the CAC is the official ID card for DoD members (i.e., U.S. military personnel, DoD civilians, eligible contractors, and members of foreign nations employed in support of the DoD mission).

Each CAC includes multiple storage areas, such as a bar code and an integrated circuit chip on the front of the card, and a bar code and magnetic stripe on the back. Various data elements, such as ID data, benefits information, organizational data, card management data, and PKI credentials (i.e., certificates and public/private key pair), are stored in one or more areas[8]. Data stored on the CAC can only be accessed through secure CAC applications.

However, the CAC is much more than an ID card. Security-enhanced engineering allows the CAC to serve as the primary interface between the user and the PKI via unclassified networked devices, such as desktops, laptops, handheld wireless devices, and peripherals, enabled for PKI use.

Enabled devices equipped with a smart card reader (and configured with the appropriate middleware application, drivers, and applicable settings) facilitate improved IA on PK-enabled networks, systems, applications, and Web servers via the digital certificates and the associated public/private key

Figure 5: *Digital Signature Process*[7]



pair embedded in the integrated circuit chip (see Figure 6).

Public Key Cryptography in the Air Force

In December 2005, the Air Force mission statement was revised to include cyberspace as a critical domain in which to fly and fight [9]. Emphasis in this domain includes, among other things, the defense and protection of critical communications assets. Air Force officials refer to cyberspace as the *new battlefield* where our adversaries operate and are gaining ground. According to Lt. Gen. Robert Elder, Jr., former Commander, 8th Air Force: "It's our most vulnerable area, and because it crosses all other domains (air, land, sea, and space), it is clearly a warfighting domain" [10].

Motivated by this new focus, the Air Force has stepped up its PKI implementation initiatives and worked diligently to become compliant with DoD directives. For example, all unclassified Air Force networks and networked applications are being public key-enabled to provide more efficient IA services and stronger authentication provisions.

Throughout the Air Force, as well as in the DoD, employees use public key-enabled applications in support of their daily activities. The rest of the federal government, defense contractors and suppliers, and allies also use PKI-enabled services. Applied uses of public key cryptography in the Air Force include:

- Identification and authentication for gaining access to unclassified networked computers, restricted Web sites, applications, and other resources (instead of usernames and passwords).
- Secure client-server transactions via the Secure Sockets Layer protocol.
- Secure financial, personnel, and contractual transactions.
- Secure unclassified messaging with authentication of originator, and confidentiality and integrity of transmitted data.
- Software (code) signing to ensure the authenticity and integrity of software obtained.
- Virtual private networking via IP security.

In Conclusion: Tangible Benefits

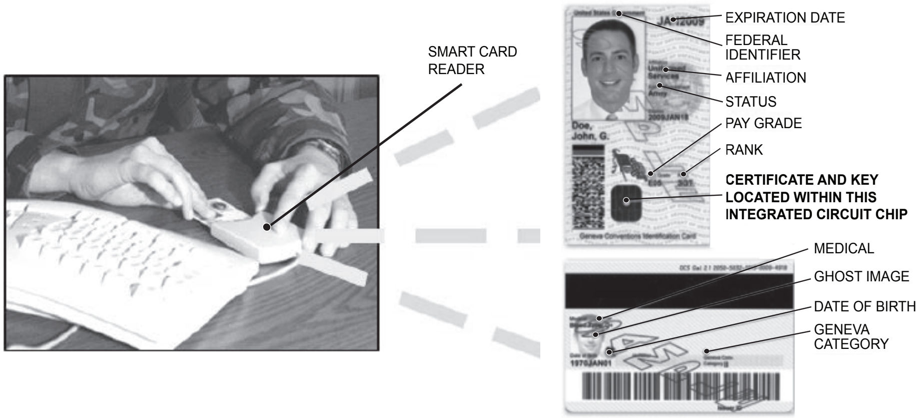
Without a doubt, PKI implementation across the DoD has attracted a significant amount of attention, primarily because of its high level of security services that support the overall IA strategy. The PKI is a sound technical solution—and is not simply a *neat* technology lacking tangible benefits. When deployed judiciously, the PKI offers certain fundamental advantages to an organization. Its capabilities help optimize workforce productivity and improve workflow efficiencies through more automated and secure business processes—including significant cost savings through the reduction of administrative overhead, reduction in the number of sign-on events required by end-users, and reduction in paper-based processes.

Knowing that virtually every day, every airman legitimately accessing DoD networks is using the PKI helps maintain confidence in critical electronic communications. One can take comfort in that.◆

References

1. National Security Agency. "Defense-in-Depth: A Practical Strategy for Achieving Information Assurance in Today's Highly Networked Environments." 2004 <www.nsa.gov/ia/_files/support/defenseindepth.pdf>.
2. Adams, Carlisle, and Steve Lloyd. *Understanding Public Key Infrastructure: Concepts, Standards, and Deployment Considerations*. Indianapolis: Macmillan Technical Publishing, 1999.
3. DoD. *Public Key Infrastructure and Public Key Enabling*. Instruction 8520.2. 2004.
4. Joint Task Force-Global Network Operations (JTF-GNO). *Tasks for Phase 1 of PKI Implementation*. Communications Tasking Order (CTO) 06-02. 17 Jan. 2006.
5. JTF-GNO. *Public Key Infrastructure Implementation, Phase 2*. CTO 07-015. 2007.
6. USAF. *Air Force Messaging*. Instruction 33-119. 2005.
7. DoD Public Key Infrastructure Program Management Office. *United States Department of Defense X.509 Certificate Policy*. Vers. 10. 2 Mar. 2009 <http://iase.disa.mil/pki/dod_cp_v10_final_2_mar_09_signed.pdf>.
8. DoD. *Smart Card Technology*. Directive 8190.3. <www.dtic.mil/whs/directives/corres/pdf/819003p. pdf>.
9. Gettle, Mitch. "Air Force Releases New Mission Statement." *Air Force Print News*. 14 Dec. 2005 <www.af.mil/information/transcripts/story.asp?storyID=123013440>.
10. Elder, Robert. *What the Air Force Is Doing for Cyber Ops and How That Supports U.S. National Interests*. Proc. of the 1st Annual Air Force Cyberspace Symposium. Shreveport-Bossier City, LA, 2007.

Figure 6: *The CAC Interfaces With the PKI Through a Smart Card Reader*



Notes

1. The PKI is not simply a product, a program, or a system—nor is it software or an application. It is a complex combination of specific hardware, specialized software, tokens, established policies, and proven procedures that *collectively* provide the ability to authenticate identities and protect valuable information through the use of unique digital certificates and key pairs.
2. The DoD PKI Chain of Trust begins at the DoD Root Certification Authority. The Root Certification Authority's public key certificate is signed by its own private key. It issues and digitally signs the certificates of the subordinate and intermediate Certification Authorities, who in turn digitally sign the user certificates they issue. The trustworthiness of each layer is guaranteed by the one before.
3. The key that is not publicly revealed is a *private key*, rather than a *secret key*. This avoids confusion with the secret key of symmetric cryptography if one thinks of two people *sharing* a secret, but a single person keeping something *private* [2].
4. Because of the processing expense in encrypting an entire message using public key cryptography, the digital signature process encrypts a digest of the message rather than the message itself.
5. For the purpose of this article, a *threat* is

Software Defense Application

The DoD implemented a PKI to provide engineered solutions that now enhance the security of networked computer-based systems. Programs and applications, which carry out or support the DoD mission, require PKI services of authentication, confidentiality, technical non-repudiation, and integrity. These services are met with an array of network security components such as standardized workstation configurations, firewalls, routers, in-line network encryptors, and trusted database servers. Public key cryptography supports and complements these component operations. As a system solution, the components share the burden of the total system security.

defined as any circumstance or event, from an authorized or unauthorized entity either inside or outside the domain perimeter, with the potential to cause harm to an information system in the form of destruction, disclosure, modification of data, and/or denial of service.

6. Encryption certificates are advertised in the DoD via the Joint Enterprise Directory Service (located at <https://jeds.gds.disa.mil>), which is the target environment, and supported by the Global Directory Service at <https://dod411.gds.disa.mil>.
7. This depiction of public key encryption and digital signatures shows text and documents as the data being protected. Public key encryption and digital signatures can be used with any type of data in a wide variety of scenarios.
8. Except for the PKI information, which is obtained from the CA, all other information about the ID card holder is obtained from the Defense Enrollment Eligibility Reporting System through the Real-time Automated Personnel Identification System. Home address and telephone number, dependent information, and medical, dental, financial, and personnel records are not stored anywhere on the CAC.

About the Authors

Susan Chandler is an associate with Booz Allen Hamilton, assigned to the Air Force PKI System Program Office at Lackland AFB, Texas. She is a 24-year veteran of the Air Force with expertise in computer operations and information systems management. She is an award-winning professional with recognized accomplishments in the areas of strategic communications and change management. Chandler has considerable experience supporting the Air Force's transformation to a more secure environment in cyberspace operations. She has a bachelor's degree in occupational education, an MBA, and is a Certified Corporate Trainer.

Booz Allen Hamilton
AF PKI SPO
4241 E Piedras DR
STE 210
San Antonio, TX 78228
Phone: (210) 925-9129
Fax: (210) 925-2644
E-mail: susan.chandler.3.ctr@us.af.mil

Jerrod Loyless is a senior software engineer for General Dynamics C4 Systems. He is the public key-enabling technical lead at the Air Force PKI System Program Office at Lackland AFB, Texas. Loyless served as an Air Force communications computer officer for six years before beginning work as a contractor and consultant. He has a bachelor's degree in computer science and a master's degree in information security, and is a Certified Information Systems Security Professional-Information Systems Security Engineering Professional, a Certified Secure Software Lifecycle Professional, and a Project Management Professional.

General Dynamics C4 Systems
AF PKI SPO
4241 E Piedras DR
STE 210
San Antonio, TX 78228
Phone: (210) 925-2073
Fax: (210) 925-2644
E-mail: jerrod.loyless@gdc4s.com

Cyberterrorism: The Threat of Virtual Warfare

Summer Olmstead and Dr. Ambareen Siraj
Tennessee Technological University

Cyberterrorism is a threat that has only surfaced worldwide in the past decade—and evidence shows that it is here to stay. With the resourcefulness of terrorists and their adaptability to ever-changing society and technology, it is a form of warfare that needs to be recognized, re-evaluated, and responded to. This article discusses cyberterrorism by exploring its definition; how its attacks on business and government entities know no boundaries; U.S. and international response; current laws; and security engineering design guidelines.

"... cyberspace is real. And so are the risks that come with it." [1]
President Barack Obama, 29 May 2009

Advances in computing technology, along with changes in society, propagated the movement of computers from secret laboratories to the average American household. The more we embrace cybertechnology, the more potential it has for being used against us. Our technical dependence is narrowing the gap between the physical world and the virtual world that surrounds us.

According to the FBI:

> ... terrorism includes the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. [2]

Cyberterrorism is an extension of terrorism, and is a result of the resourcefulness of terrorists and their adaptability to ever-changing society and technology. It is further defined as:

> The premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine agents. [3]

Cyberterrorism allows terrorists to focus their attacks through virtual warfare from anywhere in the world, at a low cost, with a high level of anonymity, and with no time or space restrictions [4]. Today, cyberterrorism includes a limitless range of crimes, such as defacing Web sites; stealing sensitive information; creating worms, Trojan horses, and viruses; and attacking infrastructures. It can arise from individuals, groups, organizations, nation-states, or countries.

The selection of tools and technologies that a cyberterrorist can utilize include malicious code, hacking, cryptography, and steganography [4]: malicious code or other hacking techniques to get access to systems, and cryptography and steganography for secret communication. Sometimes the public becomes a secondary victim when confidential information (e.g., passwords, social security numbers, credit card numbers, etc.) is stolen and used to aid virtual and real-world terrorist efforts.

"Web site defacement is the most common and extreme visual display of cyberterrorism ... although the aftermath may not always be violent, it does serve the purpose of intimidation ..."

And, of course, the future of cyberterrorism is still being determined by the actions that are being taken now, and will be taken in the near future.

The History of Cyberterrorism

Cyberterrorism has a short history: Only in the past decade have cybersecurity threats surfaced worldwide. Obvious targets of cyberterrorism consist of critical infrastructures—including transportation, electric power grids, oil and gas distribution, telecommunications, air traffic, and financial institutions.

In February 2000, a distributed denial of service (DDoS) attack was launched on popular Internet sites Yahoo, Amazon, eBay, CNN, eTrade, ZDNet, and Datek. Millions of people were unable to access services provided by these companies, resulting in monetary loss and a decline in the sense of security previously offered by these top-tier Web sites [5].

While the focus the following year became physical terrorism (9/11), an incident involving China and the U.S. in April 2001—the collision between an American surveillance plane and a Chinese fighter aircraft—was the likely culprit that initiated a series of cyberattacks and Web site defacements between the two countries [6].

Web site defacement is the most common and extreme visual display of cyberterrorism. It is a form of cyberterrorism because, although the aftermath may not always be violent, it does serve the purpose of intimidation with a political and/or social agenda. Politically motivated Web site defacement has occurred frequently in the past and present. Korean University students defaced Japanese Web sites to protest the content of Japanese textbooks [7]. In protest of the Japanese Prime Minister's visit to the Yasukuni Shrine, pro-Chinese hackers defaced Japanese Web sites. Additionally, the Pakistan-India conflict and the Israel-Palestine conflict both involved Web site defacements [6]. In 2003, Romanian hackers attacked the National Science Foundation's Amundsen-Scott South Pole Station [8]. In 2007, there were several cyberattacks on Estonia, mostly DDoS attacks on police, media, financial, and government Web sites; Estonia claimed that Russia was hacking into their systems. In August 2008, the Georgia-Russia conflict continued the pattern of Web site defacements between adversarial nations—both countries' Web sites were defaced during the period of tension over South Ossetia [9].

In early 2009, there was a report [10] that the computer systems that controlled the U.S. power grid were penetrated by foreign threats, likely Russia or China, and evidence of signature software was found. Although no monetary damage was done, the implication is inconceivable. There are many control systems (e.g., SCADA) that exist today with both cyber and physical vulnerabilities and whose unauthorized control/execution/destruction would have far-reaching effects. More recently, July 4, 2009, cyberattacks were launched at the U.S. and South Korea. The U.S. targets of the DDoS attacks included the New York Stock Exchange, Pentagon, Treasury, Secret Service, Department of Transportation, and the White House. There has been speculation that the source of the attacks was from North Korea, but there is currently no solid evidence to confirm this allegation [11]. Countries such as China, Cuba, Iran, Iraq, Libya, North Korea, Russia, Sudan, and Syria are believed to present a greater threat for potential cyberattacks than other nations.

Responding to Cyberterrorism

Cyberterrorism is real, and evidence shows that it is here to stay. While serving as U.S. Attorney General, John Ashcroft said: "One of this nation's most fundamental responsibilities is to protect its citizens, both at home and abroad, from terrorist attacks" [12]. After recognizing cyberterrorism as a genuine security concern, we as a nation should move into a more complex process of responding. In order to win this 21st century electronic war, we should adapt our practices and culture to these drastic changes brought on by the *information age*.

On May 29, 2009, President Obama announced that our digital infrastructure would be treated as a "strategic national asset" and that protecting it would be a national security priority [1]. He also announced the position of the Cybersecurity Coordinator, responsible for overseeing the government's effort to manage, protect against, and respond to cyber incidents.

The development of a new DoD command, U.S. Cyber Command (USCYBERCOM), is another response to cyberthreats by the Obama administration. The goal of the USCYBERCOM is securing our freedom of action in cyberspace [13]. The proposed headquarters would be in Fort Meade, Maryland. The implementation plan was submitted this September to Secretary of Defense Robert Gates. USCYBERCOM is planned to be at full operating capacity by October 2010.

Another response is the establishment of the Cyberterrorism Defense Analysis Center (CDAC), jointly administered by the DHS, Federal Emergency Management Agency, and Training and Exercise Integration/Training Operations [14]. The goal of CDAC is to provide comprehensive cyberterrorism training to technical personnel in critical-need infrastructures.

One method of direct response to cyberterrorism is the establishment of laws addressing cybersecurity. The U.S. government addresses threats to national cybersecurity with the Cyber Security Enhancement Act of 2002, H.R. 3482. This amendment of the Homeland Security Act calls for toughening the authority of the federal government in securing our nation's infrastructures and computer systems. It gives Internet service providers shelter from customer litigation after reporting a customer's suspicious activities and allows more extensive sentencing of cyber criminals, including up to 20 years imprisonment for harmful acts and life imprisonment for life-taking acts [4].

> *"Cyberterrorism is a global problem and as such requires global attention with initiatives to punish and deter cyberterrorists worldwide."*

Because cyberspace is borderless, attacks can originate from anywhere in the world and are not limited by physical boundaries. Cyberterrorism is a global problem and as such requires global attention with initiatives to punish and deter cyberterrorists worldwide. International responses to cyberterrorism include Singapore's Computer Misuse (Amendment) Act of 2003, Pakistan's Prevention of Electronic Crimes Ordinance of 2008, and India's Information Technology (Amendment) Act of 2008. Anyone can fall victim, either by being the target of an attack, or by being an involuntary medium (such as with botnet zombies, a network of computers controlled by malicious code). A sophisticated botnet attack can come from numerous countries at the same time. Therefore, information, intelligence sharing, and cooperation between allied countries are all the more essential to counter cyberterrorism. An example is the International Multilateral Partnership Against Cyber Threats, a coalition of 26 countries with the mission to empower the global community with the capacity to combat cyberterrorism [15].

Cyberterrorism is a complex problem that calls for a comprehensive Defense-in-Depth strategy with particular points of emphasis on prediction (proactive analysis of malicious activities to understand intent, nature, and impact for contingency planning); prevention (securing an environment to avoid penetration); deterrence (applying protection mechanisms to hurdle intruder efforts and thus causing delays in achieving a malicious goal); detection (ensuring visibility of suspicious activities); and response and recovery (reacting to security incidents by eradication, interdiction, and restoration) [16, 17]. These points of emphasis can be implemented by training, awareness, education, preventive security controls, security detection mechanisms, backup and recovery mechanisms, as well as the building of survivable systems.

The future of cyberterrorism can be negatively impacted by increasing the level of difficulty for terrorists to access vulnerabilities and decreasing the surprise and anonymity of attacks. Security engineering can help in this respect—where security is not an afterthought, but carefully dealt with from the beginning of the system life cycle. According to [18], the 10 design guidelines of security engineering are to:

1. Base security decisions on an explicit security policy.
2. Avoid a single point of failure.
3. Fail securely.
4. Balance security and usability.
5. Be aware of the possibility of social engineering.
6. Use redundancy and diversity to reduce risk.
7. Validate all input.
8. Compartmentalize assets.
9. Design for deployment.
10. Design for recoverability.

These guidelines should be part of the DoD software community culture and practice, as they hold the responsibility for development and maintenance of government software systems, in turn being the key target of cyberterrorists. Interweaving security engineering practices with designing, developing and testing systems, and management of cyberterrorism by proper risk assessment and contingency planning, can only strengthen our nation's defense for today and tomorrow.

Counter-cyberterrorism is essential. It can take the form of an average citizen who uses strong passwords for electronic accounts, a technically high-skilled *white hat* who knows how to disable malicious code, or a government official who ensures that security policies and practices are in place and properly followed. Even if cyberterrorism cannot be completely eliminated, it can mostly be prepared for, prevented to some extent, and its damage contained.

In conclusion, the absolute defense against terrorism and cyberterrorism is extremely difficult. Although cyberterrorism is currently prevailing mostly in the virtual world, technological advancements make its ability to disrupt our physical world just as possible—if not even more likely. Constantly changing technology advances our quality of life but also changes the landscape of 21st century warfare. Cyberterrorism demonstrates the ability of terrorism to adapt to the modern world and shows why it is important to continue recognizing this threat by minimizing opportunities and devoting resources to its prevention.◆

Software Defense Application

Cyberterrorism is a form of 21st century warfare that needs to be examined, especially in the DoD software community culture, where practitioners hold the responsibility for development and maintenance of government software systems, in turn being the key target of cyberterrorists. This article looks at cyberterrorism by examining its definition, history, sources, current laws, and government responses, and provides security engineering design guidelines especially useful in the DoD.

References

1. "Remarks by U.S. President Barack Obama on Securing the Nation's Cyber Infrastructure." *BBC News*. 29 May 2009 <http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/29_05_09_cyber.pdf>.
2. Code of Federal Regulations, 28 C.F.R. Section 0.85 (July 2001): 51.
3. Pollitt, Mark M. "CYBERTERRORISM – Fact or Fancy." Georgetown University. Department of Computer Science. 10 June 2009 <www.cs.georgetown.edu/~denning/infosec/pollitt.html>.
4. Kim, Jeongtae, Soyoung Park, and Tchanghee Hyun. *An Inquiry into International Countermeasures Against Cyberterrorism*. Proc. of the 7th International Conference on Advanced Communication Technology. Gangwon-Do, Korea, 2005: 432-35.
5. Biegel, Stuart. *Beyond Our Control? Controlling the Limits of Our Legal System in the Age of Cyberspace*. New York: The MIT Press, 2003.
6. Keegan, Christopher. "Cyber-Terrorism Risk." *Financial Executive* 18.8 (Nov. 2002): 35-37.
7. Bronk, Chris. "Hacking the Nation-State: Security, Information Technology and Policies of Assurance." *Information Security Journal: A Global Perspective* 17.3 (2008): 132-142.
8. "The Case of the Hacked South Pole." *Federal Bureau of Investigation Headline Archives*. 14 Apr. 2009 <www.fbi.gov/page2/july03/071803backsp.htm>.
9. Cluley, Graham. "Conflict Between Russia and Georgia Turns to Cyber Warfare." Weblog post. *Sophos*. 12 Aug. 2008 <www.sophos.com/blogs/gc/g/2008/08/12/conflict-between-russia-and-georgia-turns-to-cyber-warfare/>.
10. Ghosh, Bobby. "How Vulnerable is the Power Grid?" *Time*. 15 Apr. 2009 <www.time.com/time/printout/0,8816,1891562,00.html>.
11. Baldor, Lolita C. "White House Among Targets of Sweeping Cyber Attack." *Associated Press*. 8 July 2009 <http://abcnews.go.com/Technology/wireStory?id=8029944>.
12. Ashcroft, John. "Statement of Attorney General John Ashcroft ... on U.S. Federal Efforts to Combat Terrorism." Joint Hearing on Federal Efforts to Combat Terrorism." *The Avalon Project*. Yale Law School Lillian Goldman Law Library. 3 Apr. 2009 <http://avalon.law.yale.edu/21st_century/t_0016.asp>.
13. Gates, Robert M. U.S. Secretary of Defense. "Establishment of a Subordinate Unified Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations." Memorandum. 23 June 2009 <www.publicintelligence.net/?p=1010>.
14. Cyberterrorism Defense Initiative. 1 Sept. 2009 <www.cyberterrorismcenter.org>.
15. International Multilateral Partnership Against Cyber Threats <www.impact-alliance.org>.
16. "Defense-in-Depth Strategy Optimizes Security" *Intel Information Technology*. 1 Sept. 2009 <http://ipip.intel.com/go/3941/defense-in-depth-strategy-optimizes-security/>.
17. Siraj, Ambareen. Lecture Notes CSC 6575. Dept. of Computer Science. Tennessee Tech University. 2009.
18. Sommerville, Ian. *Software Engineering*. 8th ed. Essex, England: Addison-Wesley, 2007. 731-737.

Additional Reading

1. Anderson, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Indianapolis: Wiley Publishing, Inc., 2008.
2. Viega, John, and Gary McGraw. *Building Secure Software: How to Avoid Security Problems the Right Way*. New York: Addison-Wesley, 2001.

About the Authors

Summer Olmstead is completing her bachelor's degree in computer science at Tennessee Tech University. Her interests lie in the areas of information assurance and security.

Tennessee Tech University
P.O. Box 14734
Cookeville, TN 38505
Phone: (931) 252-7025
E-mail: smolmstead21@tntech.edu

Ambareen Siraj, Ph.D., is an assistant professor of computer science at Tennessee Tech University. She obtained her doctorate in computer science from Mississippi State University. Her research interests include information assurance and security, artificial intelligence, and software engineering.

Department of Computer Science
Tennessee Tech University
Cookeville, TN 38505
Phone: (931) 528-6081
E-mail: asiraj@tntech.edu

Certification and Accreditation of SOA Implementations: Programmatic Rules for the DoD

Anthony David Scott and Michael Malloy
Deloitte Consulting, LLP[1]

Peter Clay and Mark Masone
Deloitte & Touche, LLP

As the number of individual service-oriented architecture (SOA) projects going through the certification and accreditation (C&A) process in the DoD increases, it becomes more important to clarify the "unknowns" associated with each component. This article is a starting point for chief information officers, senior information assurance officers (SIAOs), and project managers (PMs) in the DoD, providing an overview of the challenges associated with the C&A process for SOA implementations and outlining eight rules to consider in support of a successful C&A of an SOA implementation.

When faced with the challenges of achieving system C&A in a net-centric environment, today's DoD SIAOs face a new set of challenges—such as *trusting the edge*, implementing SOA solutions, federations, varying degrees of classification levels (CLs), and multiple communities of interest (COI)—that weren't previously faced in siloed, stovepiped, vertical systems. With the discrete information systems of the past, accreditation was generally a better-defined and understood process, given the clear boundaries and finite rules governing the operating environments for such systems; today's environments are more heterogeneous and complex. The details of an SOA implementation are presently not well-defined (see Figure 1). This leaves a high degree of uncertainty and inconsistency unresolved during the first two stages of the C&A process as defined by the DoD Information Assurance Certification and Accreditation Process (DIACAP). These stages are called "Initiate and Plan Information Assurance (IA) C&A" (Stage 1) and "Implement and Validate Assigned IA Controls" (Stage 2) [1].

C&A Challenges for SOA Implementations

Unlike a vertical architecture, a horizontal architecture typically shares modules that relay data to and from other horizontal architectures, allowing the dissemination of information across COI and, at times, differing CLs. For horizontal integration, the approach toward all phases of the C&A process differs from those in a vertical integration because they involve a multiplicity of stakeholders, information systems (ISs), and environments. With that said, PMs need to pay particular attention to the first two stages of the C&A. During Stage 1, the system is registered with the DoD component program, IA controls are assigned, the DIACAP team is assembled, and the DIACAP implementation plan is initiated [1]. During Stage 2, the DIACAP implementation plan is executed, validation activities are conducted, a Plan of Action and Milestones (POA&M) is prepared, and the validation results are compiled into the DIACAP scorecard [1]. It is during these two stages that the most effective savings can be realized based on proper planning and stakeholder involvement, since the costs to remediate weaknesses are lower at this time than they will be when development is further down the road.

The DoD's increasing need to share information across boundaries provides an impetus for promoting a greater use of horizontally integrated systems, and, in turn, the ability to leverage architecture design strategies such as SOA. SOA implementations empower the DoD to achieve significant cost-savings advantages, gained by realizing economies of scale, which results from an architecture that is agile, interoperable, and open to growth. The advantages are realized by enabling information sharing and bridging disparate networks—both highly classified and open coalition.

An SOA implementation is only as secure as the most vulnerable component in the system. Clearly, a failure in effective security design and implementation can result in the significant compromise of mission-critical systems, with devastating effects at the DoD [2]. The reality of the risks, coupled with the deep functional and programmatic complexities associated with accreditation decisions in the SOA environment, have contributed to the view that achieving C&A in an effective and timely manner is an impediment to rapid Global Information Grid/net-centric SOA project rollouts when compared to C&A for traditional systems [3].

As with most high-tech companies in the private sector, the DoD's highly intelligent and well-intentioned leaders are challenged in balancing the competing demands of the *PM triad*: achieving a low-cost, on-time, and high-quality certification determination and accreditation decision for their horizontally aligned SOA implementation. At a high level, some of the programmatic issues facing the DoD are depicted in Table 1 (see next page). Not balancing the four issues could lead to an inability to achieve C&A for SOA with Full Operational Capabilities.

Several aspects of the C&A process for an SOA implementation can be reengineered. From a policy and effective practices viewpoint, a certification determination for SOA implementations is often difficult, in part due to the shifting, dynamic nature of the accreditation boundary itself [4]. Often, after going through a traditional C&A process, the scope of the final SOA implementation is reduced in functionality and implemented in such a manner that it resembles the kinds of stovepiped systems it was intended to supersede, and therefore does not reap the benefits of horizontal integration.

Figure 1: *C&A Process for Vertical and Horizontal Information Systems*

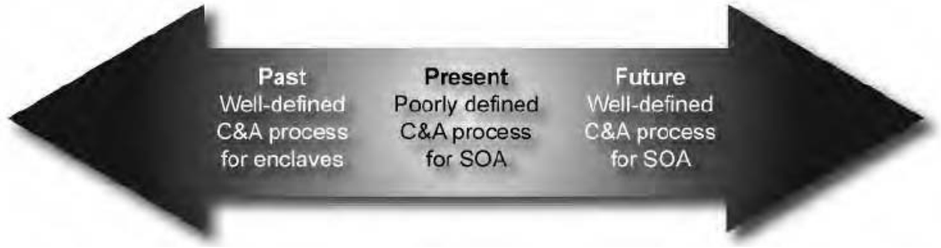


Figure 2 depicts a scenario in which the C&A process avoided complacency and facilitated an agile, robust horizontal architecture; the tendency to not accredit horizontal components limits the DoD from extracting Full Operational Capabilities for their SOA implementation.

In response to the programmatic challenges that confront DoD program managers, eight rules will be outlined (in the following section) for PMs to consider in their efforts to face and resolve the C&A challenges associated with SOA implementations. These rules are not an exhaustive list, but are rather a starting point to detail unique concerns for SOA implementations that are not typical in vertical, siloed, non-SOA implementations.

Eight Programmatic Rules to Consider

In the previous section, we identified the unique risks coupled with the C&A process for SOA associated with late identification of requirements and mitigation approaches due to the dynamic development model. We have witnessed that, all too often, the C&A process for an SOA implementation is prolonged, resulting in huge cost overruns and missed opportunities for early remediation of identified weaknesses. To be successful, there is a need for key PMs from different COIs associated with the SOA to involve themselves in sharing information and to be a part of a dedicated group committed to a successful C&A. This group must focus on consistent coordination of C&A activities and communication among stakeholders in order to fulfill the accreditation process on schedule. The following eight rules are unique to the C&A process for an SOA implementation. One would ask the DoD to consider these, in order, in their efforts to reduce risk and increase the likelihood of a successful C&A for an SOA implementation.

Rule 1: Understand SOA and C&A

As suggested earlier, today's C&A process for SOA implementations has not reached a mature state. The first and most important rule for PMs is to understand SOA and the C&A process. One of many complexities arises from the fact that the DIACAP was not authored with SOA in mind. Information superiority will emerge and productive meetings will take place only when leaders and participants understand the intersections between SOA and C&A.

When leaders do not have a grasp of SOA, unnecessary delays can occur and the functionality of the SOA implementation is at risk of being marginalized or lost completely. If necessary, appropriate briefings or training should be considered as a prerequisite for participating decision-makers.

Rule 2: Embrace Risk Management, Identification, and Planning

Each IS in the DoD is unique and has uncertainties associated with it. Risk management should be performed over the lifetime of the accreditation decision to assess and monitor risk. A POA&M should be used to mitigate the risk of an incident occurring. At the least, the POA&M should detail the priorities of the risk, status, and due date. If PMs do not plan for risk, it is very likely that they will be forced into addressing unexpected issues that may ultimately result in cost overruns and/or undesirable accreditation decisions.

In addition to risk management, risk identification and planning must also be addressed. For C&A of an SOA implementation, risk identification and planning is more involved and less understood than C&A of traditional stovepiped architecture.

Table 1: *Programmatic Issues Facing the DoD*

Scope	Quality	Cost	Schedule
• Dynamic system boundary • Dynamic classification levels • Dynamic services	• Systems not performing as designed • Confusion about who owns services • Managing multiple COI services • Lack of innovation • Lack of training • Nonadherence to policy • High repetition	• Poor execution of acquisition process (DoD 5000 series) • Poor estimation of level of effort (LOE) • Poor capitalization on economics of scale	• Delay in authorization to operate (ATO) • Complacency towards C&A change

It is imperative that the C&A process for SOA implementations is accurately budgeted and appropriately managed to promote reduced risk and avoid cost overruns as SOA components are reworked to address interim weaknesses. From a DoD policy stance, when an SOA implementation is accredited correctly, IA costs go down by an order of magnitude, as do the risks. On paper, the reduction in cost and apparent increase in security is impressive. However, the results are elusive: The IA risk profile of the system actually increases because new security vectors are created within the boundary of the SOA implementation. Extending security beyond what policy mandates and implementing proactive, repeatable procedures into the C&A process should contribute to ensuring a(n) 1) reduction in risk of budget overruns, 2) consistency in planning, and 3) increase in the dissemination of information pertaining to existing risks. Since the systems development life cycle of a horizontal system is heavily dependent on constituents and external partners, unique considerations exist for the C&A process for SOA implementations that rely heavily on teaming and communicating with external parties and internal constituents. Budget overruns can be reduced when security is fully integrated throughout the systems development life cycle and repeatable processes are fully documented and appropriately executed.

If adverse risk is not properly characterized, the C&A process could be forced to continue past the expected timeframe (i.e., the ATO could be pushed back). As a result, resources supporting the C&A process would need to stay on longer, preventing them from being productive on other projects and, if the contract is not fixed price, causing cost overruns on the C&A project. When resources are not able to join other projects, it causes a chain reaction: The critical path of the organization is impacted, and the overall functionality of the organization is reduced. As a result, the project might be completed at a date later than planned, costs might overrun, and the organization's service reputation might slip.

Rule 3: Understand that Schedule and LOE Estimations are Different

Unlike stovepiped systems, an increased LOE needs to be dedicated to educating the IA community on SOA, SOA risks, and SOA protections. As a result, the schedule and LOE is different than that of a traditional vertical IS; it will increase. It has been seen with many new technologies attempting to go through the C&A process in the DoD. For example, in the wireless arena, much effort has gone into educating the IA community on the risks and protections needed to achieve secure wireless. Similarly, accomplishing the same goals for SOA will tend to increase the required LOE and schedule for the C&A of SOA implementations, at least initially.

In addition to educating the IA community, procedural issues can slow down the C&A process. At present, SOA services themselves cannot be accredited, although there are several proposals and notional constructs on how it could be done currently circulating throughout the DoD community. The future accreditation of services is, by itself, a major topic and not limited to considerations for schedule and LOE.

Rule 4: Plan for Future External Relationships

The goals of SOA include improved collaboration, interoperability, horizontal integration, efficiency, and agility. These goals can be realized only through expanding the IS's boundary to encompass the SOA's multiple accreditation components in a consistent, reusable form.

It is important that PMs plan ahead for interoperability with IA controls of future SOA implementations. Future SOA implementations and shared services with external third parties will have configurations and IA controls that might cause interoperability; anticipation and planning should help avoid this.

PMs for a new SOA must communicate early with owners of other enclaves and COI; the goal is to drive existing ATO dates, anticipate changes to current configurations, and consider controls used in SOA implementations still on the horizon. The goal should be for the overall level of risk associated with the system to be recognized as *acceptable* to the IS that will be exchanging services with the new IS being accredited. It is critical to gather stakeholder risk issue input prior to implementation, otherwise belated input may become a problem for the SOA C&A on the whole.

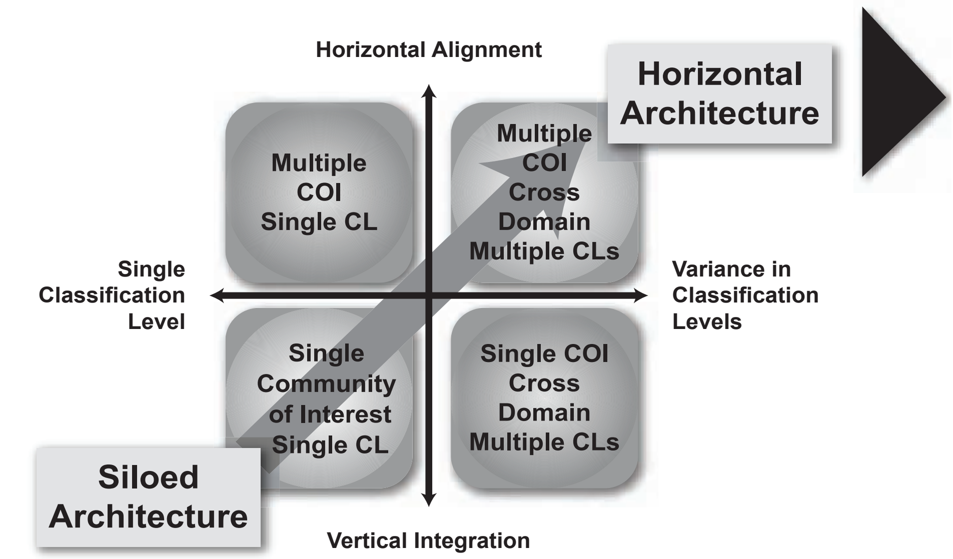

Horizontal Alignment
Horizontal Architecture
Multiple COI Single CL
Multiple COI Cross Domain Multiple CLs
Single Classification Level
Variance in Classification Levels
Single Community of Interest Single CL
Single COI Cross Domain Multiple CLs
Siloed Architecture
Vertical Integration

Figure 2: *Sample C&A Process*

Rule 5: Plan for Present External Relationships

When operating an IS, the DIACAP limits the time that an accreditation decision is valid based on the severity categories (indicating the risk level associated with the security weakness), expressed as category (CAT) I, CAT II, and CAT III, where CAT I is more severe than CAT III. Sections 4.9 and 6.3.3.2.6 [1] detail the duration associated with Interim Authorization to Operate (IATO), ATO, Interim Authorization to Test (IATT), or Denial of Authorization to Operate decisions. Table 2 provides a summary of the duration of each of these decisions; the duration of an ATO has direct cost and schedule impacts.

Since PMs are responsible for reducing risk and balancing scope, cost, schedule, and quality, an understanding of the duration of each accreditation decision and knowledge about when the ATOs expire is mandatory. This knowledge should also be included in the LOE estimates. As external third-parties' ATOs expire or new service components are added to SOA systems, each service component will have its own corresponding ATO date. If overlooked, these subordinate dates could creep up and possibly impact the overall ATO for the SOA itself.

Each type of accreditation decision (i.e., ATO, IATO, IATT) has a corresponding duration in which the decision is valid. Obviously, longer accreditation periods are preferable in order to reduce the frequency of the accrediting process, which can be costly and impact the system's availability.

The following three factors drive the necessity and urgency behind planning for present-day external third-party relationships:

1. **ATO expiration of existing SOA implementations.** For an existing SOA implementation with shared services from external third parties, it is important to keep track of expiring ATOs to help drive the reaccreditation process, in turn helping ensure shared service availability.
2. **Configuration changes of existing SOA implementations.** For an existing SOA implementation with configuration changes from external third parties, it is important to drive the reaccreditation process, in turn helping ensure shared service availability.
3. **Opportunities to capitalize on economies of scale.** During the C&A process, teaming with organizations might unveil opportunities to eliminate redundant activities and save hard and soft costs.

PMs can begin to experience a decrease in cost overruns by identifying the steps

Table 2: *Duration of the C&A Process*

Type	Authorization Termination Date	CAT I	CAT II	CAT III
ATO	<= 3 years of authorization	No ATO	ATO — must be corrected in 180 days	ATO
IATO	Reset <= 180 of authorization	No ATO	ATO — must be corrected in 360 days	IATO
IATT	Special Case	Special Case	Special Case	Special Case

involved in the C&A process that involve both the organizations they exchange services with, as well as their own organization. Every cost associated with the C&A should be identified, line by line. Once the cost categories have been identified, opportunities for cost savings should be analyzed [5]. An example of cost savings includes teaming with neighboring programs to reduce duplication and eliminate waste. Once waste is identified, PMs should determine what can be realistically eliminated [6].

Rule 6: Use eMASS, DIACAP KS, and Other Cost-Effective or Free Tools

As discussed earlier, PMs should use existing infrastructure tools and knowledge to reduce cost and make quick, measurable progress. Leveraging the DoD's Enterprise Mission Assurance Support Service (eMASS) tool will help automate the DIACAP process via reports generation and tracking of IA controls. The results of the certification determination or accreditation decision are provided automatically on an electronic DIACAP scorecard [7].

DoD organizations can use eMASS for free [8]. Residual costs might include the training of personnel to use eMASS and time to perform data entry. Training and usage costs depend on the number of individuals assigned eMASS roles, locations, facilities, and capabilities. Typically, the cost of training ranges from $5,000 to $10,000 for up to 30 people. Additionally, the Defense Information Systems Agency (DISA) hosts a free quarterly training course, running two full business days.

Like eMASS, DIACAP Knowledge Service (KS) is an information repository that should be leveraged when executing the C&A process for SOA implementations [7]. DIACAP KS holds a wealth of information and up-to-date resources from practitioners that help to facilitate knowledge transfer for the C&A process. For example, the KS houses best practices, lessons learned, guidance documents, schematics, and many other resources to facilitate the DIACAP process [8]. Like eMASS, there is no cost in using KS.

In addition to eMASS and KS, the following are also free IA tools. They should be considered for use during the C&A process for SOA implementations, although many PMs find the tools helpful to support substantially more:

1. **Vulnerability Management System.** A tool developed by the DoD to assess risk during accreditation activities across programs and systems for all types of vulnerabilities.
2. **DoD IT Portfolio Repository – Department of Navy**. A tool developed by the Department of Navy that serves as a technical database of Federal Information Security Management Act assessments.
3. **Gold Disks.** A tool developed by DISA to run vulnerability scans for specific systems, available through the DoD's Information Assurance Support Environment.
4. **Cyber Security Assessment and Management System.** A Web-based tool developed by the Department of Justice that facilitates the C&A process.

Rule 7: Do Not Let Complacency Undermine Horizontal Integration

The DoD systems development environment has been stovepiped for many years. Complacency in moving forward with effective deployment of horizontal integration strategies could ultimately limit the possibilities of an SOA-based enterprise software feature set. Instead of true integration, the DoD could instead wind up with a new series of well-intentioned, but still stovepiped, systems that lack the kind of net-centric data integration and interoperability that has become synonymous with SOA. Complacency results from many things; however, when technology is not well-understood, advanced, or cutting-edge, feature sets may be compromised and replaced with a system that is more familiar, better understood, and more closely resembles the risk profile of past ISs that were accredited. Understandably, a loss of feature sets due to budgetary or mission issues is a business reality. However, if a loss of feature sets is due to an inclination toward not wanting to upset the status quo, it may result in lost opportunity. At a large enough scale, complacency could undermine horizontal integration and the DoD's goal of communicating military intelligence throughout the Global Information Grid and onto the battlefield.

> *"Governance, interoperability, situational awareness, and data aggregation should be key elements in a fluid maintenance approach to SOA component ATOs."*

Rule 8: Strive for a Fluid Maintenance Phase

Maintaining ATO and performing periodic reviews is the fourth phase of the DIACAP process. This compliance phase is an ongoing process that involves vulnerability scans, penetration tests, IA controls verification, scorecard updates, IA controls modifications, security vulnerabilities mitigations, configuration management, and compliance with existing controls. As SOA implementations mature in the DoD, so too will the lessons learned, along with the deepening understanding of SOA's unique IA implications. Governance, interoperability, situational awareness, and data aggregation should be key elements in a fluid maintenance approach to SOA component ATOs.◆

References

1. DoD. *DoD Information Assurance Certification and Accreditation Process*. Instruction 8510.01. 28 Nov. 2007 <www.dtic.mil/whs/directives/corres/pdf/851001p.pdf>.
2. DoD. *Data Sharing in a Net-Centric Department of Defense*. Directive 8320.02. 23 Apr. 2007 <www.dtic.mil/whs/directives/corres/pdf/832002p.pdf>.
3. Brown, Jeb, and Stacy Spence. "Draft IBM Perspective on Information Assurance Challenges in Service Oriented Architectures." IBM Working Paper. 6 Mar. 2007.
4. "Service-Oriented Architecture." *Wikipedia*. 26 Jan. 2009 <http://en.wikipedia.org/wiki/Service-oriented_architecture>.
5. Dubbeling, Scott, Glenn Richardson, and Brian Siegel. "Strategic Cost Reduction in the Department of Defense." Deloitte eLearning Course. 3 May 2007.
6. "Can We Afford Our Own Future?" *Deloitte Consulting LLP*. 23 Mar. 2009 <www.deloitte.com/dtt/cda/doc/content/us_a&d_project%20management%20report-pov(1).pdf>.
7. Turner, Glenda, et al. "Net-Centric Assured Information Sharing – Moving Security to the Edge Through Dynamic Certification and Accreditation." *IA Newsletter* 8.3. Winter 2005/2006 <http://iac.dtic.mil/iatac/download/Vol8_No3.pdf>.
8. "DIACAP Frequently Asked Questions (FAQs)." *Defense Information Systems Agency*. 4 Apr. 2008 <http://iase.disa.mil/diacap/diacap-faq.pdf>.

Note

1. This publication contains general information only and is based on the experiences and research of practitioners from Deloitte & Touche LLP and Deloitte Consulting LLP, two separate subsidiaries of Deloitte LLP. Deloitte is not, by means of this publication, rendering business, financial, investment, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

Software Defense Application

During the C&A process for SOA implementations, the DoD community is given a second chance to solve technical issues that involve software interoperability and security. When the C&A process for an SOA implementation is prolonged, huge cost overruns and missed opportunities can result. This article is a resource and provides the DoD software community with techniques and methodologies to consider in their efforts to avoid unnecessary cost overruns associated with the C&A process for SOA implementations. It ties software selection and security architecture to upfront planning, helping PMs as they streamline the C&A process and reduce costs, risks, and the time to implement—while increasing mission effectiveness.

Additional Resources

1. Committee on National Security Systems. *National Information Assurance Glossary*. Instruction No. 4009. June 2006 <www.cnss.gov/Assets/pdf/cnssi_4009.pdf>.
2. Project Management Institute. *A Guide to the Project Management Body of Knowledge*. 3rd ed. Newtown Square, PA: Project Management Institute, 2004.
3. DoD. *DoD Information Technology Security Certification and Accreditation Process Application Manual*. Instruction 8510.1-M. July 2000.
4. DoD. *DoD Information Technology Security Certification and Accreditation Process*. Instruction 5200.40. Dec. 1997.
5. Ross, Ron, et al. *Guide for the Security Certification and Accreditation of Federal Information Systems*. National Institute of Standards and Technology. Special Publication 800-37. May 2004 <http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>.
6. National Security Agency – National Security Telecommunications and Information Systems Security Committee. *National Security Telecommunications and Information Systems Security Policy No. 11: National Policy Governing the Acquisition of Information Assurance and IA-Enabled Information Technology Products*. June 2003.
7. Director of Central Intelligence. *Protecting Sensitive Compartmented Information within Information Systems*. Directive 6/3. 24 May 2000.
8. DoD. *Guidance for Implementing Net-Centric Data Sharing*. Directive 8320.02-G. 12 Apr. 2006 <www.dtic.mil/whs/directives/corres/pdf/832002g.pdf>.
9. Williams, Peter, and Tiffani Steward. "DoD's Information Assurance Certification & Accreditation Process." *Defense AT&L* (Sept.-Oct. 2007).

About the Authors

Anthony David Scott is a manager for Deloitte Consulting with 10 years of cybersecurity experience in the commercial and federal sectors. Scott continues to be an active participant in the federal community, publishing and holding workshops at the IEEE, Computer Security Institute, DoD, and at DHS conferences. He is a licensed professional engineer and a Certified Information Systems Security Professional. Scott holds a master's degree in electrical and computer engineering from Georgia Tech and an MBA from Columbia University.

Deloitte Consulting, LLP
1750 Tysons BLVD
McLean, VA 22102
Phone: (703) 251-1696
Fax: (703) 332-7108
E-mail: davidscott@deloitte.com

Michael Malloy is an analyst with Deloitte Consulting and works primarily in the public sector with the DoD. He specializes in custom system development and has strong knowledge regarding SOA and related topics. Malloy graduated from Boston College with a bachelor's degree in computer science and mathematics.

Deloitte Consulting, LLP
1001 G ST
STE 900 W
Washington, D.C. 20001
Phone: (443) 694-1545
Fax: (202) 661-1802
E-mail: mimalloy@deloitte.com

Peter Clay is a senior manager with 16 years of IA experience in the federal and financial market sectors. He currently specializes in DoD information security governance and is the federal representative in the Deloitte & Touche Vulnerability Management Center of Excellence. Clay is also a Certified Information Systems Security Professional.

Deloitte & Touche, LLP
1750 Tysons BLVD
McLean, VA 22102
Phone: (703) 220-3531
Fax: (703) 894-9191
E-mail: peclay@deloitte.com

Mark Masone is a senior manager with nine years experience as an IA professional working closely with federal and DoD organizations. Most notably, he supported the Office of the Assistant Secretary of Defense for Networks and Information Integration on DIACAP implementation efforts. He has supported the authorship of the DIACAP while managing its two components: KS and eMASS. Masone is a Certified Information Systems Security Professional, a Certified Information Privacy Professional/Government, and a Certified Secure Software Lifecycle Professional. He has a bachelor's degree from Virginia Tech and master's degree in systems engineering from George Washington University.

Deloitte & Touche, LLP
1750 Tysons BLVD
McLean, VA 22102
Phone: (703) 251-1843
Fax: (703) 894 -9191
E-mail: mmasone@deloitte.com

Preparing for an Internal Assessment Interview

Jim O'Brien
Office of Enterprise Development, U.S. Department of Veterans Affairs

With proper training and preparation, most professionals can successfully negotiate an internal assessment. This article presents practical survival tips on how to effectively participate, knowing how an assessor typically behaves during an interview and knowing how one can best demonstrate compliance to standards.

When the assessor knocked on the door, the developer greeted him with "Come in."

The assessor began by introducing himself and explaining the purpose of the assessment. Senior management had requested an objective assessment to determine the level of compliance with corporate policies, processes, and procedures. When the developer seemed a little nervous, the assessor assured her that her project team members had done just fine.

After some conversation about the project and work that she was performing, the assessor asked to see the project plan and quality plan that guided the project work.

The developer produced the two documents. However, without warning, she tore up both documents, threw them in the trash can, and said "That's what I think of the assessment!"

Initially, the assessor was shocked at the reaction. "We can handle this one of two ways," said the assessor calmly. "We can stop right here, or we can take a five-minute break, you can reproduce the documents, and we can make like this incident never happened."

The two colleagues agreed to start over. The woman passed the assessment with a couple of minor notations.

Later in the conversation, the developer explained that she was ill when the assessment training was offered and pleaded with her project manager to get the training. The developer took pride in her work and did not want to be the team member that failed the assessment. As we learned later, it was an unnecessary panic.

Most people do a good job and have nothing to fear from the arrival of an assessor. However, a few tips on how to prepare for an assessment can go a long way. Preparing management and technical staff to participate in an assessment is a critical ingredient for the success of any quality management system.

The Office of Enterprise Development (OED) for the U.S. Department of Veterans Affairs (VA) has successfully prepared management and technical staff by addressing what may occur during some types of assessment interviews.

Management and technical staff want to know what is expected of them during an assessment interview.

> *"Though internal assessors may not be bound by the same formalism of external assessors, they are truly professionals who determine the level of compliance to the organization's quality management system ..."*

Types of Assessors

Two types of assessors may come knocking—an external assessor or an internal assessor.

An external assessor is frequently portrayed as someone who comes from out of town and carries a briefcase. The external assessor assesses compliance to a standard or set of standards external to the organization, such as ISO 9001-2000, CMMI®, the IT Infrastructure Library, the FDA, and so forth. In today's competitive marketplace, it is becoming more common for organizations to build their quality management systems in such a way as to satisfy multiple external standards. Thus, the external assessor is typically an expert in one or more standards.

By comparison, an internal assessor is a company employee or contractor who may inhabit the next cubicle and stays around after the completion of the internal assessment. The internal assessor knows the work, the culture, and sometimes the people. The internal quality assessor typically performs internal assessment duties in addition to their work assignments.

Though internal assessors may not be bound by the same formalism of external assessors, they are truly professionals who determine the level of compliance to the organization's quality management system and, in some circumstances, prepare the organization for external compliance or certification.

Assessor Interview Techniques

The internal assessor structures the assessment interview by stating the endorsement of management, explaining the purpose of the assessment, and scheduling the interview at a time and place agreeable to the assessor and assessee. Since so many employees today are distributed geographically, it is necessary to conduct some assessment interviews via teleconferencing across multiple time zones.

During the actual interview itself, the person being assessed can expect the internal assessor to restate the purpose and scope of the assessment. Essentially, the assessment focuses on what's in and what's out of assessment consideration.

The internal assessor invites the assessee to speak about work practices and may ask questions, such as:

- What do you do?
- What are your roles and responsibilities?
- What software development life cycle does your project follow?
- What procedures guide your work activities?
- Does your project have a software development or a project management plan?

At some point, the conversation will

® CMMI is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

turn towards standards compliance. The internal assessor may ask to see:

- The procedures that guide your work.
- Your documentation and records.
- Your requirements and design model.
- Your plans and reports.
- Any special processes (i.e., patch review or billing procedures).

The internal assessor verifies compliance by obtaining *objective evidence*. Objective evidence includes documentation, artifacts, tools, media, and records that demonstrate compliance to the quality management system, and, in this case, policies, directives, processes, and procedures. The internal assessor looks for requirements documentation, test plans, meeting minutes, and installation guides (as specified by the standard) as objective evidence that the standard is being followed. Opinion, statements, and hearsay do not suffice as objective evidence.

The internal assessor may also dig deeper and request very specific information, such as:

- Minutes from a particular meeting.
- A record of acceptance (e-mail).
- Results from a test.
- A review meeting log.
- A controlled version of a template.

A seasoned internal assessor may select certain minutes, reports, or tests randomly and will resist any attempt to be led.

Finally, when it is appropriate, the internal assessor may give some indication of how you did during the interview. If the internal assessor finds compliance, they may say so. Providing immediate informal feedback can foster goodwill between the internal assessor and the assessee. However, informal feedback may not be possible in every situation. The internal assessor will deliver the assessment findings during the closing meeting and in the final report.

Management and Technical Staff

As management and technical staff, you may be asking yourself, "That's nice to know what the internal assessor does, but what do I do during the assessment?"

Here are a few tips on how to participate in an assessment interview.

1. **Answer the questions directly and honestly.** Your responsibility is to provide the information requested. If you do not understand the question, then say so. If the question does not apply to you or your project, then say so. Any attempt to withhold information or to deceive only hinders the desire to improve processes and how work gets done. If you do not know the answer to the question, say that you don't. In this case, honesty is the best policy.
2. **Do not volunteer information.** Answer the question and only the question. Resist any temptation to expand or go beyond the question asked. The internal assessor will notice when conversation is diverted or too much information is given. Simply put, let the internal assessor lead; do not volunteer unrequested information.
3. **Provide objective evidence of compliance.** Demonstrate that you are following current standards and practices by presenting relevant documentation and records. As Sergeant Joe Friday used to say on *Dragnet*, "Just the facts, ma'am."

   In our earlier-mentioned assessment, the internal assessor asked to see the project's Vision document; the project manager stated that he didn't have it. The internal assessor was puzzled by this remark and inquired, "Didn't I see one in the project documentation you submitted?" The project manager turned to his computer, searched the project documentation, and—sure enough—found it. With that document, the project manager demonstrated compliance to the standard.
4. **Ask others for help.** Remember that it is the project being assessed, not the individuals. If you do not know something and you think that other project members do, you can point the internal assessor to others. A project manager or test lead may possess a wonderful grasp of the project but may not know where a particular record is stored. You can ask others for help.
5. **Have a reasonable amount of time.** Sometimes you just cannot find the requested process, procedure, or record during the assessment interview. You should be given a *reasonable amount of time* to produce the item. If you can show the requested item, even after the interview, the internal assessor will evaluate the evidence and consider the project compliant.

Coaching

More and more organizations are encouraging assessors to function as process improvement coaches. Two goals of any assessment are to 1) help employees work more efficiently and effectively and 2) improve the processes that guide how work is done. In some quality management systems, when an assessor comes across best practices, he or she records these in the assessment findings.

At the conclusion of one assessment interview, an assessment participant asked about the existence of testing templates. The assessor said that he was taking off his assessor's hat and putting on his coaching hat, then explained that the XYZ project Test Plan contained appendices with templates for test cases, test suites, and test reports. Both walked over to view the test templates. The assessor identified the test templates as a best practice and connected one project with another.

By collecting and communicating best practices, the assessor and assessment participant help to improve the quality of an organization's products and processes.

Initially, a quality assessment may seem like a scary event. However, with a little quality preparation training and confidence in one's own professionalism, an assessment can be a valuable time to demonstrate how your work practices support the business goals of your company.

When an internal assessor comes knocking, say "Come in"—then say what you do, do what you say, and prove it. In other words, know the quality standards that guide your work, follow the standards, and demonstrate compliance when asked.◆

About the Author

Jim O'Brien is a senior process engineer with Electronic Data Services and the OED process improvement program for the VA. O'Brien, a Certified Lead Assessor, has trained quality assessors for the VA and two major telecommunications providers. He obtained both his bachelor's degree and Masters of Sacred Theology from St. Mary's Seminary and University in Baltimore. He is currently assisting with the development of the OED's process and product quality assurance program.

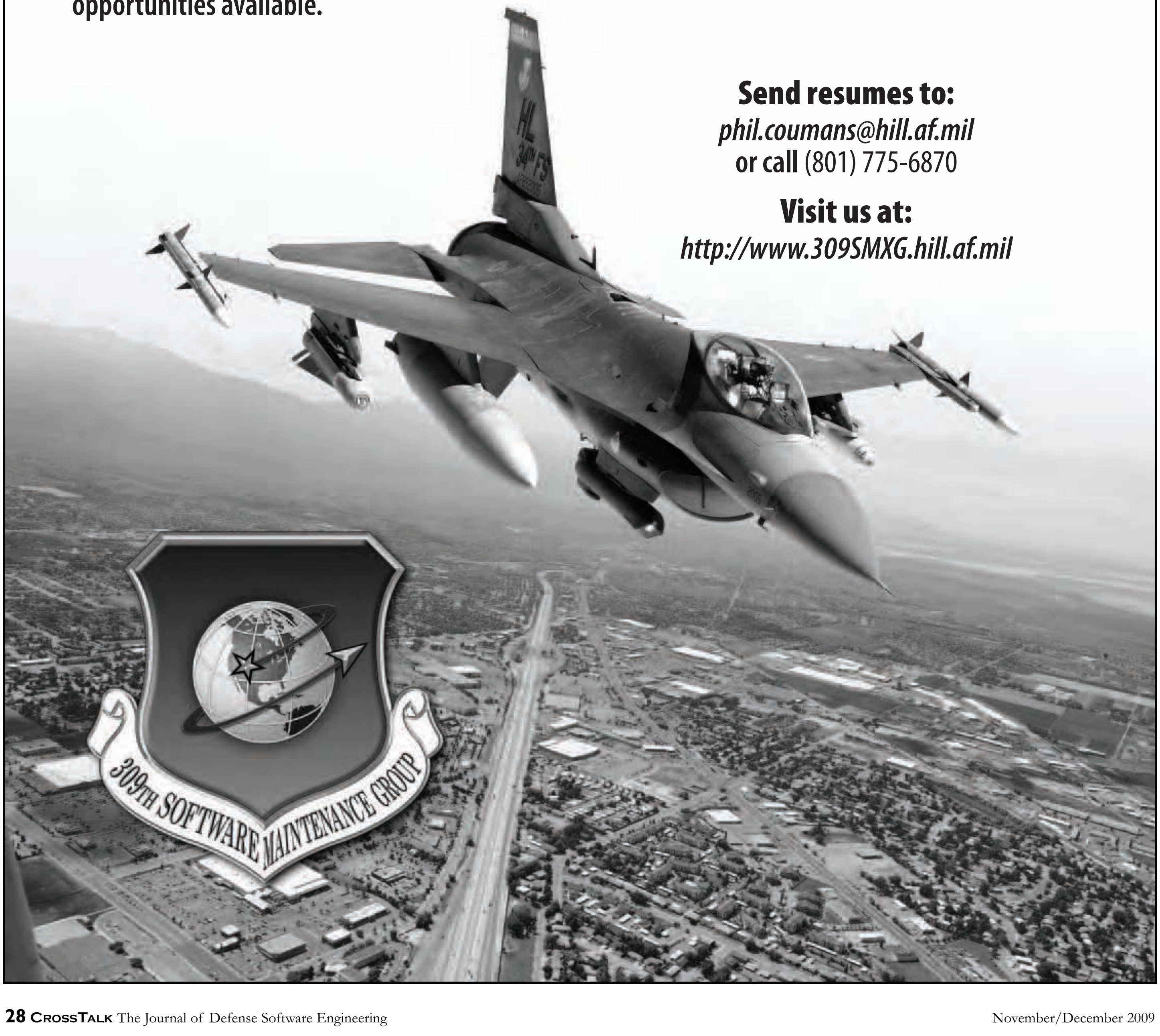
OED – VA
Process Management Service
Birmingham Office of Information
STE 201
Birmingham, AL 35209
Phone: (205) 943-2449
E-mail: jim.obrien@va.gov

WANTED

Electrical Engineers and Computer Scientists
Be on the Cutting Edge of Software Development

The Software Maintenance Group at Hill Air Force Base is recruiting **civilian positions** *(U.S. Citizenship Required)*. Benefits include paid vacation, health care plans, matching 401k, tuition assistance and time off for fitness activities. **Become part of the best and brightest!**

Hill Air Force Base is located close to the Wasatch and Uinta mountains with many recreational opportunities available.



Send resumes to:
phil.coumans@hill.af.mil
or call (801) 775-6870

Visit us at:
http://www.309SMXG.hill.af.mil

Web Sites

Georgia Tech Wearable Motherboard

www.gtwm.gatech.edu

You've read MAJ Phillip G. Burns' article on the Combat Wireless Health Monitoring System, now learn more about the Georgia Tech Wearable Motherboard (GTWM)—the "smart shirt" prototype that started it all. Learn more about the garment that uses optical fibers to detect bullet wounds and special sensors that interconnect to monitor the body's vital signs during combat conditions. Also learn more about why the GTWM is needed in combat; next-generation GTWMs; the project team and the impact of their research; and national media coverage on the technology.

Information Assurance Support Environment – Public Key Infrastructure (PKI)

http://iase.disa.mil/pki

After reading Susan Chandler and Jerrod Loyless' article on the DoD's PKI—a service of products which provide and manage X.509 certificates for public key cryptography—you may want to visit the DoD's "one-stop shop" for information assurance and PKI knowledge and training. You can receive guidance on policy issues; get information on the DoD PKI's around-the-clock Help Desk; connect with the PKI Certificate Policy Management Working Group; download training guides, memos, and other PKI documents; receive DoD PKI online training; read government memoranda and training guides regarding PKI; link to other Web sites of interest; and learn about the External Certification Authority Program. There is also information on the DoD's expansion of their Secret Internet Protocol Router Network (SIPRNet), and how SIPRNet smart cards will increase security levels.

Remarks by the President on Securing Our Nation's Cyber Infrastructure

www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

Summer Olmstead and Dr. Ambareen Siraj—in *Cyberterrorism: The Threat of Virtual Warfare*—delve into an issue that President Barack Obama addressed in his May 29, 2009 speech covering the great promise but great peril of cyberspace. President Obama's speech covers cybercrime in its many forms: identity theft, privacy violations, the economic risks to e-commerce, ATM robberies, and stolen intellectual property. He also addresses national security issues and the recent cyber intrusion into our power grid. The President's main focus, though, is our military networks, which have faced the most serious cyber incidents and infections via malware. After discussing these issues, the President outlines a new approach and a range of actions in five key areas.

Information Assurance Support Environment – DITSCAP Transition to DIACAP

http://iase.disa.mil/diacap

In this issue's *Certification and Accreditation of SOA Implementations: Programmatic Rules for the DoD*, the authors discuss the DoD Information Assurance Certification and Accreditation Process (DIACAP), a process to ensure that risk management is applied on Information Systems from an enterprise view. This Web site gives an overview of DIACAP; provides guidelines in the transitioning from the DoD's Information Technology Security Certification and Accreditation Process (DITSCAP); offers access to the signed DIACAP in its entirety as well as to National Information Assurance Certification and Accreditation Process Instruction; and links users to online DIACAP training.

Interview: John G. Grimes

http://defensesystems.com/Articles/2008/11/Interview-with-John-Grimes.aspx

Assistant Secretary of Defense for Networks and Information Integration/DoD CIO (and frequent CrossTalk contributor), the Honorable John G. Grimes, believes that organizations have to work together for interoperability. In this interview from *Defense Systems* magazine, Grimes discusses issues including the alignment of the military services' IT infrastructures, the challenge of information sharing among government agencies, and the threat of cyberattacks. He also discusses the DoD's movement to service-oriented architecture, which is providing great opportunities for the DoD to quickly deploy Web services that make information available across organizational boundaries.

The Lean Systems Engineering (LSE) Working Group

http://cse.lmu.edu/about/graduateeducation/systemsengineering/INCOSE.htm

The goal of the LSE Working Group is to strengthen the practice of SE by exploring and capturing the synergy between traditional SE and Lean. Through the Web site, the group: applies the wisdom of Lean thinking into SE practices, people, processes, and tools for the most effective delivery of value to program stakeholders; formulates the body of knowledge of LSE; and develops and disseminates training materials and publications on Lean SE within the International Council on Systems Engineering community, as well as with industry and academia. Learn more about the group—its members, history, publications, accomplishments, and mission—as well as receive access to several resources detailing what Lean SE is all about.

Software Engineering Process Group (EPG) Guide

www.sei.cmu.edu/reports/90tr024.pdf

Read the guide that revolutionized software EPGs and told readers that "it takes tremendous energy to counter our own and others' resistance." Even after 19 years, Priscilla Fowler and Stan Rifkin's work is still a must-read for anyone wanting to establish a software EPG. Emphasizing the "what" over the "how," the guide offers a basic introduction to the subject and provides guidance for initiating and sustaining an improvement program in an organization. The guide is as much concerned with the human side of stimulating a higher quality process as with the technology of improved processes.

Coming Events

January 18-21

11th Annual Lean Six Sigma and Process Improvement Summit 2010

Orlando, FL

www.leansixsigmasummit.com

January 20-22

37th Annual ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages

Madrid, Spain

www.cse.psu.edu/popl/10

January 25-28

Network Centric Warfare 2010

Arlington, VA

www.ncwevent.com

February 24-25

AFCEA Homeland Security Conference

Washington, D.C.

www.afcea.org/events/homeland

February 28-March 3

17th Annual Network and Distributed System Security Symposium

San Diego, CA

www.isoc.org/isoc/conferences/ndss/10/

April 26-29

22nd Annual Systems and Software Technology Conference

Salt Lake City, UT

www.sstc-online.org

Coming Events: Please submit coming events that are of interest to our readers at least 90 days before registration. E-mail announcements to: <marek.steed.ctr@hill.af.mil>.

Letter to the Editor

Dear CrossTalk Editor,

The July/August 2009 article *Why Software Requirements Traceability Remains a Challenge* was spot-on in regards to the multiple difficulties faced in the utilization of the requirements traceability in practice.

Andrew Kannenberg and Dr. Hossein Saiedian have correctly identified the burden that the production of this artifact puts on project teams with no discernible benefits to the individuals or to the teams. No amount of training and policy can change that.

One creates an artifact in order to use it. I have not seen, in 18 years of software development, anyone actually using the requirements traceability matrix or other incarnations thereof.

For requirements traceability to be useful, all the tools used in the software development value chain ought to be able to produce or consume requirements traceability data in a transparent manner. That is, the requirements management tools, the modeling tools, the integrated development environments, the testing tools, the configuration management tools, and the project management tools must be able to support the tracing of the same (software) requirement through the life cycle of the system being built or maintained transparently and easily.

—Babak Makkinejad, Ph.D.
Services Information Developer, HP
babak.makkinejad@hp.com

Reality Check or Parody Bit?

It started in the '60s with Allen Funt's *Candid Camera*: the concept that real life is more interesting than fantasy. No need for celebrities, scripts, or big budgets to attract viewers. Chuck Barris upped the ante in the '60s and '70s with *The Dating Game, The Newlywed Game*, and *The Gong Show*, all exploiting our social quirks.

In the '90s, *The Real World*'s "seven strangers living together and having their lives taped" ushered in a reality TV explosion: With one part voyeurism, two parts duplicity, and three parts *schadenfreude*, you have a natural rubbernecker. Reality TV introduced us to interesting careers like that of the ice road trucker, avian vomitologist, derrickhand, maggot farmer, saucier, and catfish noodler ... but no engineers.

Why is that? If viewers can stomach Kate nagging Jon (or her eight kids) or Ramsey's kitchen expletives, surely they could bear brunch with Booch, tea with Torvalds, or cocktails with Cockburn. Think of the possibilities to promote our industry with software engineering versions of reality TV shows.

We could start with *Big Brother*, a "Fly-on-the-Wall" (FotW) show where twelve Agile software engineers move into a government project to develop the National Medical Records Database with no outside help. Watch tensions rise as a National Information Czar drops daily obstacles on the team: CMMI Level 5, Six Sigma, Lean, an unexpected thumb drive ban[1], limited Internet access, staff meetings, and Foreign Object Damage training. Each week an engineer is discharged from the team based on compliance, seniority, and staff meeting attendance.

On our version of *The Real World*, a project manager is coerced into joining his subordinates as a contributing engineer. Watch in amazement as he tries to boot up test stands and simulators. See paralysis set in during critical design review. Tempers flare when peer reviews turn to payback. Tears flow during budget cuts and schedule accelerations.

Closing out the FotW genre, we have *Engineer vs. Wild*, where, each week, a software engineer is dropped into the middle of a start-up company and asked to develop a company-wide knowledge management system with a laptop, an Internet connection, and a can of Mountain Dew. Watch as he or she rubs two modules together to create a parser and erects a makeshift database from an abandoned VisiCalc application.Cringe as he or she battles exposure to hackers, constant schedule heat, and budget dehydration. Cheer as he or she accomplishes his or her first back-up recovery.

In the "vocational" genre, we could start with engineering's version of *Dirty Jobs*. Mike Rowe demonstrates jobs engineers loathe: configuration management, sales, documentation, supervision, and quality assurance—all death knells to an engineer's career.

Next, we could offer a "vocational" quartet starting with *Deadliest Catch*, in which CEOs bid for the talent of a prima donna architect experienced in three design methods, six programming languages, and four software development environments, and speaks fluent CMMI, PSP^{SM}, and Earned Value. This is followed by *Wail Wars*, where current project engineers welcome said prima donna architect with distractions, ploys, and impediments to foil his attempt to whip them into shape. Then there's *Ax Men,* where the project manager—who never wanted to hire said prima donna architect—consults with the CEO, CFO, human resources, and legal council to determine whether to sack the architect or the rebellious engineers. The final of the four shows would be *Dog the Bounty Hunter*, where said prima donna architect, whose first name happens to be Dog, writes a book titled "Prima Donna Design: Architecture for Those Who Can." We follow Dog as he travels the country hunting companies he can fleece through lectures, workshops, and consulting gigs.

Switching channels we find a surplus of "reality-competition" shows to work with, starting with the slightly re-named *Project Runaway.* Here engineers are given a runaway project with no oversight, schedule, or quality assurance. The first to bankruptcy wins an autographed Heidi Klum poster. *Shear Genius* pits engineers against each other as they cut, trim, shape, and transform mainframe legacy code into an iPhone app. In *Hell's Kitchen*, programmers try to find a software bug nestled inside two million lines of undocumented spaghetti code. In *America's Got Talent*, project managers are asked to develop software-intensive systems with no H-1B visas, foreign workers, or offshore outsourcing. *Wipeout* pits system administrators against software engineers for control of the software development environment while *Fear Factor* is a fun little show that forces engineers to use their own products in near-death situations. *The Biggest Loser* tests software engineers' ability to provide minimal functionality for the most money. In *The Mole*, anti-process engineers are planted inside Engineering Process Groups to sabotage quality assurance ratings before they are discovered. Finally, engineering teams match wits in *The Weakest Link* as they transfer critical data across random platforms, data links, and protocols like an electronic hot potato. Lose the data and "you are the weakest link ... goodbye!"

Finally we offer the "makeover" genre. In *Trading Spaces*, real-time programmers are assigned to data processing centers with abundant memory, storage, and resources while database programmers are assigned to a real-time software intensive system with cycle constraints, interrupts, and memory paging. Each tries to improve the other's system and then critiques the results. In *Supernanny*, top-notch consultants race to be the first to convert talented cowboy programmers to PSP and TSP^{SM}. *Peer Eye for the Late Guy* drops in on team interventions, disguised as peer reviews, to help procrastinating engineers meet milestones and deadlines. And *What Not to Wear* ... for engineers, the possibilities are endless.

Engineering reality TV may not be the answer. Most reality shows grow more scripted and less real with success. We are probably better off sticking with *MythBusters*. That show captures the heart of an engineer: showing how something works, watching it being built, and then blowing it up! Don't let success taint your engineering skills. Undergo regular reality checks to assure your parity bit is true and not a parody bit.

—Gary A. Petersen
Arrowpoint Solutions, Inc.
gpetersen@arrowpoint.us

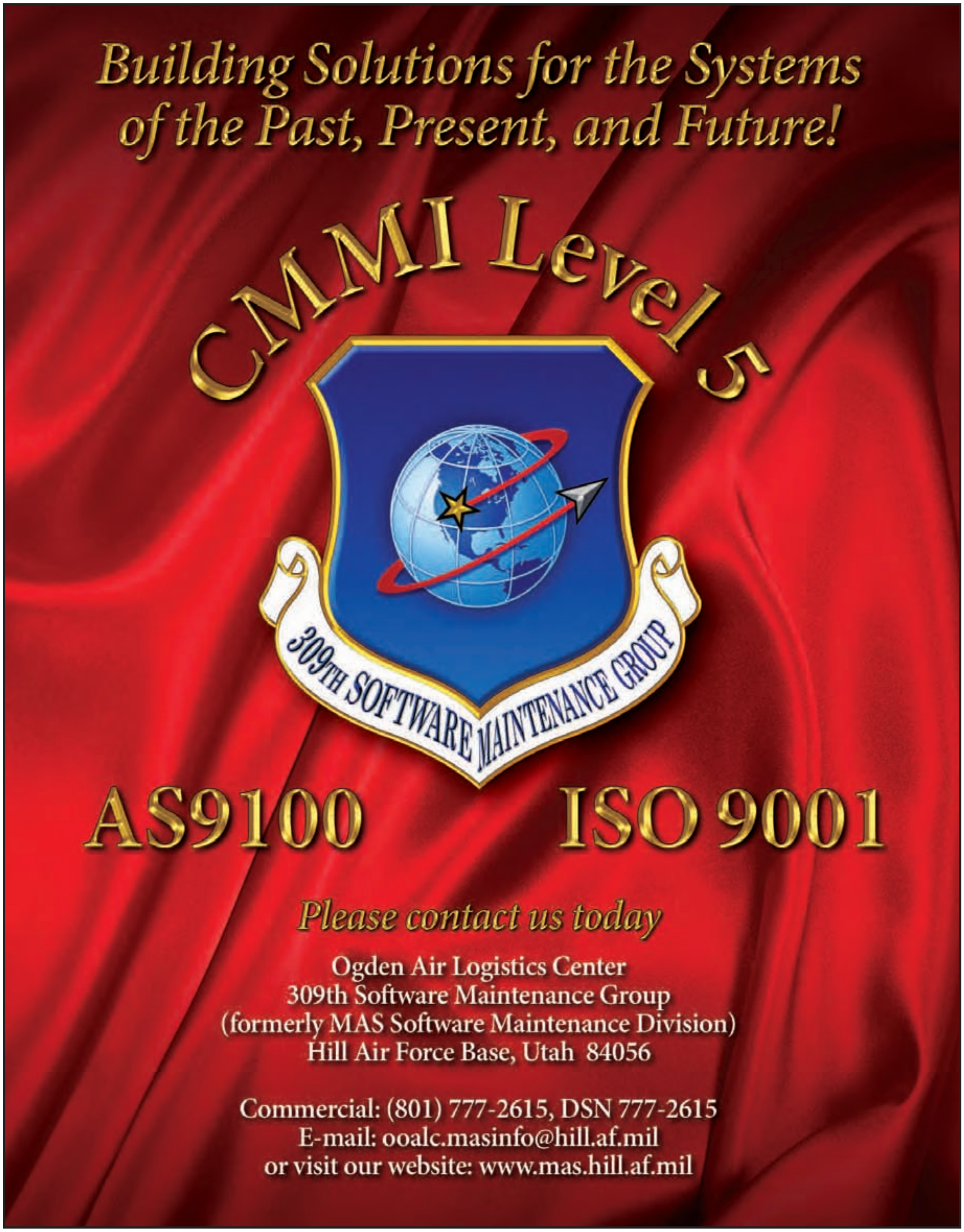
Note

1. For those not working with or for the government, you may be surprised to find that this actually happened. See: <www.nextgov.com/nextgov/ng_20090217_6795.php>.

^{SM} TSP and PSP are service marks of Carnegie Mellon University.

CrossTalk / 517 SMXS/MXDEA
6022 Fir AVE
BLDG 1238
Hill AFB, UT 84056-5820

PRSRT STD
U.S. POSTAGE PAID
Albuquerque, NM
Permit 737


Building Solutions for the Systems
of the Past, Present, and Future!
CMMI Level 5
309TH SOFTWARE MAINTENANCE GROUP
AS9100
ISO 9001
Please contact us today

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

NAVAIR

309TH SOFTWARE MAINTENANCE GROUP

U.S. DEPARTMENT OF HOMELAND SECURITY

CrossTalk thanks
the above
organizations for
providing their support.